openstax™

Foundations of

Infor-mation Sys-tems

Foundations of Information Systems

SENIOR CONTRIBUTING AUTHOR

DR. MAHESH S. RAISINGHANI, TEXAS WOMAN'S UNIVERSITY

openstax™

OpenStax
Rice University
6100 Main Street MS-375
Houston, Texas 77005

To learn more about OpenStax, visit https://openstax.org.
Individual print copies and bulk orders can be purchased through our website.

COLOR PAPERBACK BOOK ISBN-13	**978-1-711472-95-9**
B&W PAPERBACK BOOK ISBN-13	**978-1-711472-94-2**
DIGITAL VERSION ISBN-13	**978-1-961584-63-1**
ORIGINAL PUBLICATION YEAR	**2025**

1 2 3 4 5 6 7 8 9 10 CJP 25

OpenStax

OpenStax provides free, peer-reviewed, openly licensed textbooks for introductory college and Advanced Placement® courses and low-cost, personalized courseware that helps students learn. A nonprofit ed tech initiative based at Rice University, we're committed to helping students access the tools they need to complete their courses and meet their educational goals.

Rice University

OpenStax is an initiative of Rice University. As a leading research university with a distinctive commitment to undergraduate education, Rice University aspires to path-breaking research, unsurpassed teaching, and contributions to the betterment of our world. It seeks to fulfill this mission by cultivating a diverse community of learning and discovery that produces leaders across the spectrum of human endeavor.

RICE

Philanthropic Support

OpenStax is grateful for the generous philanthropic partners who advance our mission to improve educational access and learning for everyone. To see the impact of our supporter community and our most updated list of partners, please visit openstax.org/foundation.

Arnold Ventures
Chan Zuckerberg Initiative
Chegg, Inc.
Arthur and Carlyse Ciocca Charitable Foundation
Digital Promise
Ann and John Doerr
Bill & Melinda Gates Foundation
Girard Foundation
Google Inc.
The William and Flora Hewlett Foundation
The Hewlett-Packard Company
Intel Inc.
Rusty and John Jaggers
The Calvin K. Kazanjian Economics Foundation
Charles Koch Foundation
Leon Lowenstein Foundation, Inc.
The Maxfield Foundation
Burt and Deedee McMurtry
Michelson 20MM Foundation
National Science Foundation
The Open Society Foundations
Jumee Yhu and David E. Park III
Brian D. Patterson USA-International Foundation
The Bill and Stephanie Sick Fund
Steven L. Smith & Diana T. Go
Stand Together
Robin and Sandy Stuart Foundation
The Stuart Family Foundation
Tammy and Guillermo Treviño
Valhalla Charitable Foundation
White Star Education Foundation
Schmidt Futures
William Marsh Rice University

CONTENTS

Preface

About OpenStax

OpenStax is part of Rice University, which is a 501(c)(3) nonprofit charitable corporation. As an educational initiative, it's our mission to improve educational access and learning for everyone. Through our partnerships with philanthropic organizations and our alliance with other educational resource companies, we're breaking down the most common barriers to learning. Because we believe that everyone should and can have access to knowledge.

About OpenStax Resources

Customization

Foundations of Information Systems is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 (CC BY NC-SA) license, which means that you can non-commercially distribute, remix, and build upon the content, as long as you provide attribution to OpenStax and its content contributors, under the same license.

Because our books are openly licensed, you are free to use the entire book or select only the sections that are most relevant to the needs of your course. Feel free to remix the content by assigning your students certain chapters and sections in your syllabus, in the order that you prefer. You can even provide a direct link in your syllabus to the sections in the web view of your book.

Instructors also have the option of creating a customized version of their OpenStax book. Visit the Instructor Resources section of your book page on OpenStax.org for more information.

Art Attribution

In *Foundations of Information Systems,* art contains attribution to its title, creator or rights holder, host platform, and license within the caption. Because the art is openly licensed, anyone may reuse the art as long as they provide the same attribution to its original source.(Commercial entities should contact OpenStax to discuss reuse rights and permissions.) To maximize readability and content flow, some art does not include attribution in the text. If you reuse art from this text that does not have attribution provided, use the following attribution: Copyright Rice University, OpenStax, under CC BY-NC-SA 4.0 license.

Errata

All OpenStax textbooks undergo a rigorous review process. However, like any professional-grade textbook, errors sometimes occur. In addition, the wide range of evidence, standards, practices, data, and legal circumstances in computer science change frequently, and portions of the text may become out of date. Since our books are web-based, we can make updates periodically when deemed pedagogically necessary. If you have a correction to suggest, submit it through the link on your book page on OpenStax.org. Subject matter experts review all errata suggestions. OpenStax is committed to remaining transparent about all updates, so you will also find a list of past and pending errata changes on your book page on OpenStax.org.

Format

You can access this textbook for free in web view or PDF through OpenStax.org, and for a low cost in print. The web view is the recommended format because it is the most accessible—including being WCAG 2.2 AA compliant – and most current. Print versions are available for individual purchase, or they may be ordered through your campus bookstore.

About *Foundations of Information Systems*

Foundations of Information Systems provides students with the ability to understand the concepts of IS, including hardware, software, database management systems, and data networks. The teaching is based on the ACM/IEEE/AIS curriculum standards for information systems (IS2020) that allow institutions to use the content for the purposes of accreditation for ABET, AACSB, and ACBSP. The openly licensed resource is grounded in concepts that cross both functional and operational areas to develop student knowledge in transactional, decisional, and collaborative business processes. Specifically, students will be able to understand and apply basic concepts associated with the collection, processing, storage, distribution, and value of information—and how IS professionals provide support to management, customers, and suppliers of the enterprise. Driven by competencies that correlate to knowledge, skills, and dispositions, the book is an asset for 2-year and 4-year information systems programs and to use in general education courses in business and computing.

Foundations of Information Systems is intended to be a high-quality, introductory text that provides students with foundational knowledge of global information systems while preparing them to engage with more complex problems and digital technologies. The IS resource appeals to multiple audiences of learners and instructors teaching courses in information technology and those teaching in a comprehensive program in any specialty, including health information systems and business information systems. The book is designed to closely align with international standards and real-life skills needed by employers, while providing a scholarly perspective that encourages students to explore the digital world from a systems design perspective.

Coverage and Scope

Foundations of Information Systems provides a cohesive narrative flow that brings content to life through application, examples, and exercises. The text is based on the recommended Foundations of Information Systems 2020 Curriculum. The topics and format are aligned with the suggested first course in the program of IS2020 and include additional topics organized and recommended by instructors across in 2-year, 4-year, and general education programs around the world. Content is organized under headings and subheadings to allow for structured reading and comprehension, with pedagogical features placed to provide breaks and reinforce concepts. Appropriate visuals complement and illustrate key points in the narrative and draw students into the material.

Foundations of Information Systems begins with an overview of hardware, software, and system identification, and ends with ethical considerations in using such technology as machine learning, artificial intelligence, and other newly developed technologies.

Pedagogical Foundation and Features

Foundations of Information Systems is designed to engage students through a combination of practical, real-world applications and thought-provoking scenarios that promote critical thinking and a deeper understanding of core concepts. The pedagogical approach is centered on making information systems relevant and accessible for students from diverse backgrounds. To support this vision, the textbook incorporates several key features:

- **Future Technology** features present newer, emerging, and rapidly changing technologies such as artificial intelligence, machine learning, virtual reality, and augmented reality, and how these technologies fit into the information systems domain.
- **Global Connections** features highlight information systems and technology on a global scale. This feature highlights real IS cases from organizations around the world and describes global technology.
- **Ethics in IS** features highlight ethical issues related to the concepts, skills, and activities being taught in the course. These discuss real-world cases, dig deeper into ethical considerations, and present ethical dilemmas for students to think through.
- **Careers in IS** features introduce students to careers in information systems, including those in high demand, such as health care, data analytics, cybersecurity, cloud computing, business analytics, financial analytics, and more. In addition, this feature offers insight into specialty areas, certifications, and other learning and experience opportunities to enhance career options.
- **Link to Learning** features provide a very brief introduction to online resources—videos, interactives,

articles, and other engaging resources that are pertinent to students' exploration of the topic at hand.

Overall, these features are integrated throughout the textbook to foster active learning, critical thinking, and an appreciation for the practical applications of information systems. By connecting theory to practice and encouraging students to explore real-world issues, *Foundations of Information Systems* provides a meaningful and supportive learning experience that equips students with the knowledge and skills necessary for success in their academic and professional journeys.

Answers to Questions in the Book

The end-of-chapter Check Your Understanding and Application Questions are intended for homework assignments or classroom discussion; thus, student-facing answers are not provided in the book. For end-of-chapter Review Questions, the book's Answer Key provides students with answers to about half of the assessments so they can self-check their work as they study. All assessment answers and sample answers are provided in the Instructor Answer Guide, for instructors to share with students at their discretion, as is standard for such resources.

About the Author

Senior Contributing Author

Senior contributing author: Dr. Mahesh S. Raisinghani

Dr. Mahesh S. Raisinghani is a professor of Management Information Systems at Texas Woman's University's (TWU's) MAK College of Business and Entrepreneurship, and an Affiliate Professor at TWU's Woodcock Institute for the Advancement of Neurocognitive Research and Applied Practice. He is also a Senior Fellow of the Higher Education Academy in the U.K., and the Director of Strategic Partnerships for the Association of Information Systems' SIG-LEAD. He earned his MBA from the University of Central Oklahoma; M.S. in Information Systems, and Ph.D. in Information Systems and Strategic Management from the University of Texas at Arlington.

Dr. Raisinghani was awarded the Distinguished Research Award by the Association of Business Information Systems in 2022 and 2024; Global Educator Award from X-Culture in 2022, 2023, and 2024; Information Systems Audit and Control Association (ISACA's) Excellence in Education award in 2021; Outstanding Organizational Service award from the Global Information Technology Management Association in 2018; and TWU's 2017 Innovation in Academia award, among other awards. He was also awarded the 2017 National Engaged Leader Award by the National Society of Leadership and Success; and the 2017 Volunteer Award at the Model United Nations Conference for his service to the Youth and Government by the Model United Nations Committee.

Dr. Raisinghani serves as the Editor-in-Chief of the *International Journal of Web-based Learning and Teaching Technologies*. He has published over a hundred manuscripts in peer-reviewed journals in MIS, national and international conferences, and book series; edited eight books; and consulted for a variety of public and private organizations. He has been involved in many large, medium, and small business technology strategy and innovation projects for companies in several countries across various industries. He has extensive experience with corporate training and has developed and delivered training and mentoring programs for the top corporate education providers.

Dr. Raisinghani has served as a consultant and conducted research as part of a project that received Phase 1, and Phase 2/2B grants from the National Science Foundation. He has also served as a subject matter expert reviewer in technology and commercialization for the National Science Foundation for the last 25 years. Dr. Raisinghani serves as a Board Member for the Global Information Technology Management Association; an Advisory Board Member for Harvard Business Review and X-Culture.org; and an advisor for the National Society of Leadership and Success and World Affairs Council.

Contributing Authors

Amal Alhosban, University of Michigan

Dax Bradley, Miller-Motte College

Wade Chumney, California State University, Northridge

Nicole Dhanraj, University of Maryland Global Campus

Sherita Freeman, North Carolina Agricultural and Technical State University

James Gibbs, Louisiana State University Shreveport

Sean Petty, Paradise Valley Community College

Karen Srba, University of Maryland Global Campus

Ayushi Tandon, Trinity College, Dublin, Ireland

Reviewers

Peter Appiahene, University of Energy and Natural Resources

Tammie Bolling, Pellissippi State Community College

Quiana Bradshaw, St. Francis College

Mariya Breyter, New York University

Joseph Budu, Ghana Institute of Management and Public Administration

Alaina Desjardin, Franklin University

Sukhen Dey, University of the Cumberlands

Dina Engel, New York University

Betty Fitte, Tidewater Community College

David Fogarty, New York University and Columbia University

Janos Fustos, Metropolitan State University of Denver

Graham Gal, University of Massachusetts Amherst

Jim Gerland, University at Buffalo and Buffalo State University

Rhonda Gilreath, Tiffin University

David Hearst, Florida Atlantic University

Angela Heath, Baptist Health Systems

Rania Hodhod, Columbus State University

Benita Hubbard, Capella University

Andrew Hurd, Empire State University

James Hyatt, University of the Cumberlands

Jessica Kong, University of Washington

Michael MacLeod, The University of Texas at San Antonio

Thomas Moore-Pizon, University of South Florida

Sai Mukkavilli, Georgia Southwestern State University

Garrett Pierman, Florida International University

Caryl Rahn, Florida International University

Vincent Sanchez, Florida International University

Rakshit Shah, EdgeVerve Ltd

Jayesh Soni, Florida International University

Abdel Toure, Estrella Mountain Community College

Charlyne Walker, Florida International University

Jingnan Xie, Millersville University

Ning Xie, Florida International University

Additional Resources

Student and Instructor Resources

We have compiled additional resources for both students and instructors, including Getting Started Guides, an instructor's answer guide, test bank, and image slides. Instructor resources require a verified instructor account, which you can apply for when you log in or create your account on OpenStax.org. Take advantage of these resources to supplement your OpenStax book.

Instructor's answer guide. Each component of the instructor's guide is designed to provide maximum guidance for delivering the content in an interesting and dynamic manner.

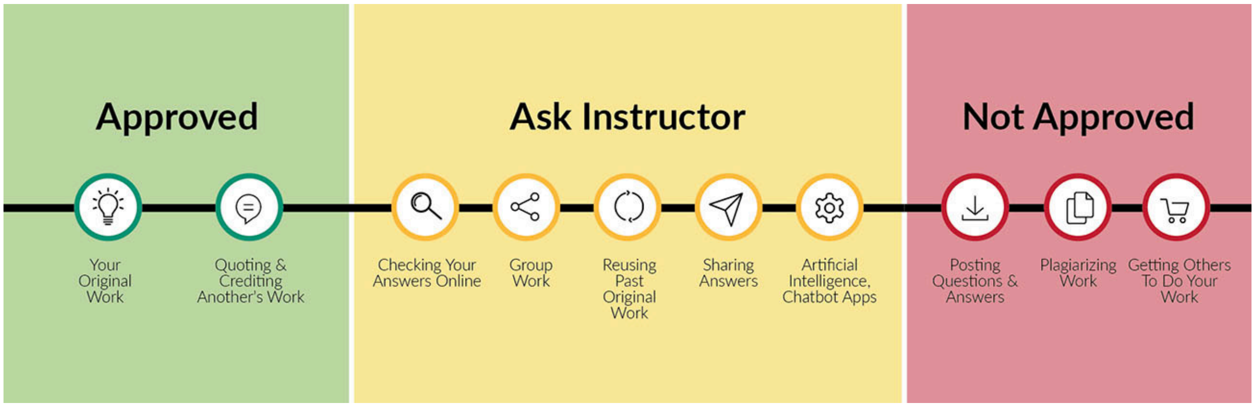
Test bank. With hundreds of assessment items, instructors can customize tests to support a variety of course objectives. The test bank includes review questions (multiple-choice, identification, fill-in-the-blank, true/false), short answer questions, and long answer questions to assess students on a variety of levels. The test bank is available in Word format.

PowerPoint lecture slides. The PowerPoint slides provide learning objectives, images and descriptions, feature focuses, and discussion questions as a starting place for instructors to build their lectures.

Academic Integrity

Academic integrity builds trust, understanding, equity, and genuine learning. While students may encounter significant challenges in their courses and their lives, doing their own work and maintaining a high degree of authenticity will result in meaningful outcomes that will extend far beyond their college career. Faculty, administrators, resource providers, and students should work together to maintain a fair and positive experience.

We realize that students benefit when academic integrity ground rules are established early in the course. To that end, OpenStax has created an interactive to aid with academic integrity discussions in your course.



Visit our academic integrity slider (https://view.genial.ly/61e08a7af6db870d591078c1/interactive-image-defining-academic-integrity-interactive-slider). Click and drag icons along the continuum to align these practices with your institution and course policies. You may then include the graphic on your syllabus, present it in your first course meeting, or create a handout for students. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

At OpenStax we are also developing resources supporting authentic learning experiences and assessment. Please visit this book's page for updates. For an in-depth review of academic integrity strategies, we highly recommend visiting the International Center of Academic Integrity (ICAI) website at https://academicintegrity.org/ (https://academicintegrity.org/).

Community Hubs

OpenStax partners with the Institute for the Study of Knowledge Management in Education (ISKME) to offer Community Hubs on OER Commons—a platform for instructors to share community-created resources that support OpenStax books, free of charge. Through our Community Hubs, instructors can upload their own materials or download resources to use in their own courses, including additional ancillaries, teaching material, multimedia, and relevant course content. We encourage instructors to join the hubs for the subjects most relevant to your teaching and research as an opportunity both to enrich your courses and to engage with other faculty. To reach the Community Hubs, visit www.oercommons.org/hubs/openstax.

Technology partners

As allies in making high-quality learning materials accessible, our technology partners offer optional low-cost tools that are integrated with OpenStax books. To access the technology options for your text, visit your book page on OpenStax.org.

1

Fundamentals of Information Systems

Figure 1.1 Information systems are an integral part of our lives. Organizations rely on them to manage data, produce goods and services, and compete successfully in marketplaces big and small. (credit: modification of work "Infoeko2" by "Deeply"/Wikimedia Commons, CC0 1.0)

Chapter Outline

Introduction

What comes to mind when you think about information systems? In what ways do you think they affect your life? You might be surprised to find out that information systems have an impact on your life and career whether you realize it or not.

In general, an information system is a set of components that helps gather, analyze, maintain, and distribute data. The components of information systems include people, the system's hardware and software, networks, data, and the procedures used to process the data and maintain the system.

The fields of information systems (IS) and information technology (IT) overlap, and sometimes the terms are used interchangeably. However, the sole focus of the field of IT is technology, meaning the processes necessary to establish and maintain computer systems, networks, and applications. Although the field of IS is concerned with technology, the focus is broader to include the people who are part of system processes. It is a vital tool used by all types of organizations to conduct business and participate in the marketplace, whether local or global.

To put this in perspective, consider the village of Pathanamthitta in Kerala, India. The village has limited resources, and during the COVID-19 pandemic, residents' access to health care was even more limited. To improve the health of the vulnerable geriatric population and protect them from the disease, researchers created a mobile phone app for symptom reporting, telehealth, and assessments. Approximately 60 percent of the geriatric population used the app, and the mobile health project thereby allowed for improved health care for the community.[1] This is information systems in action, using technology and information to help address concerns from the COVID-19 pandemic.

1.1 Introduction to Information Systems

Learning Objectives

By the end of this section, you will be able to:

- Define the key concepts in information systems
- Discuss the historical evolution of information systems
- Describe the components, elements, and operations of information systems

It's helpful to understand the relationship between information systems and related fields. Computer science is the discipline that provides foundations for the theories and technology necessary for computing systems. Information technology (IT) implements and maintains those computer systems. Information systems, our area of focus, uses those systems to process and manage information.

Key Concepts in Information Systems

An **information system** is a set of interconnected components that integrate the collection, processing, storage, and distribution of data, information, and digital products in order to support decision-making, coordination, control, analysis, and visualization in an organization. These systems play an important role in managing and facilitating various business processes and can also be used in individuals' personal lives.

The **field of information systems (IS)** is a dynamic industry, evolving and depending on technological advancements. It intersects with business, computer science, and management, playing a critical role in enhancing organizational efficiency, productivity, and competitiveness. When organizations have robust information systems, they are more capable of planning strategically to gain a competitive edge and achieve success.

Components of an Information System

As shown in Figure 1.2, an information system typically consists of five key components: hardware, software, data, people, and procedures.

1 Geethu Mathew, Nooh Bava, Aby Dany Varghese, Abey Sushan, and Anoop Ivan Benjamin, "Project *Vayoraksha*: Implementation of Novel mHealth Technology for Healthcare Delivery during COVID-19 in Geriatric Population of Kerala," *Indian Journal of Medical Research*, 159, 3–4 (July 19, 2024): 289–297, https://doi.org/10.25259/IJMR_62_23

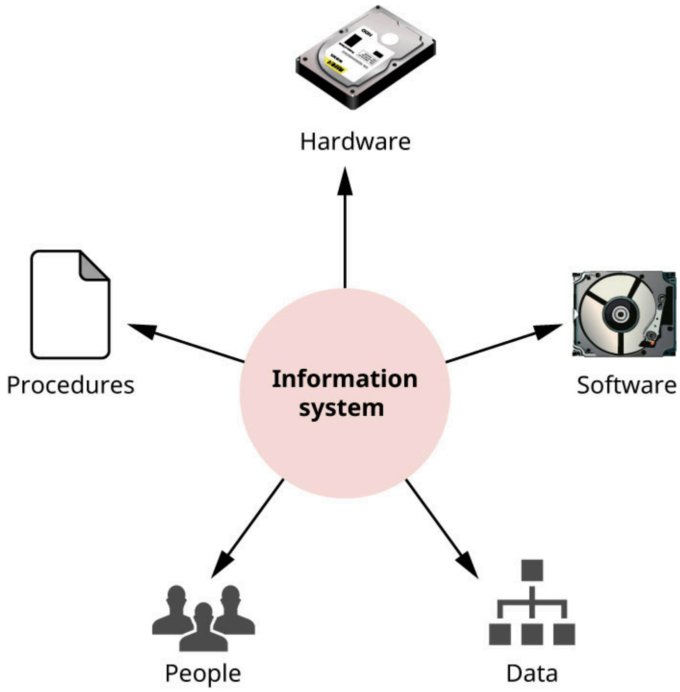


Figure 1.2 Typically, an information system includes people, as well as hardware, software, data, and procedures. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Before looking closely at each component to understand what it entails and why it is important in IS, let's start with a brief overview of the five components.

- The physical devices, such as computers, servers, networks, and storage devices, that are used to collect, process, and store data are called **hardware**.
- The programs and applications that run on the hardware, enabling users to perform specific tasks, are called **software**. Software can range from operating systems and database management systems to specialized business applications.
- The raw facts and figures that are processed and turned into meaningful information are called **data**. The facts that we use to learn and understand people, places, and things make up **information**. Information is raw data that have been processed and manipulated to give context and meaning. Once data are processed into information, we can use that information personally and professionally. We read or listen to books, watch videos on social media, stream a television show, follow road signs, browse online shopping sites, and interact with information we find on the internet or in the world around us. We use databases to organize and store this data efficiently.
- A Set of instructions and rules that governs the use of the hardware, software, and data components is known as a **procedure**. Standard operating procedures ensure consistency and reliability in the use of information systems.
- Individuals who use the information system, including end users who input and retrieve data in the system, as well as information technology (IT) professionals who design, develop, and maintain the system, are the people who make up an information system.

LINK TO LEARNING

If you are interested and want to learn more about career opportunities in IS, search "information systems careers" online and explore the dozens of websites with IS career details. This article provides information about [career paths and salary (https://openstax.org/r/109ISCareers)](https://openstax.org/r/109ISCareers) and includes links to online higher education institutions that have related degrees. An online search can find other websites that provide helpful information about IS careers, including the general skills required, types of organizations that hire IS professionals, and what students can expect if they pursue a career in IS.

Types of Information Systems

As shown in Figure 1.3, information systems can be categorized into different types based on their scope and functionality. Executive information systems are used by an organization's executive staff, decision support systems are used by senior managers, management information systems are used by middle managers, and transaction processing systems are used by frontline workers.

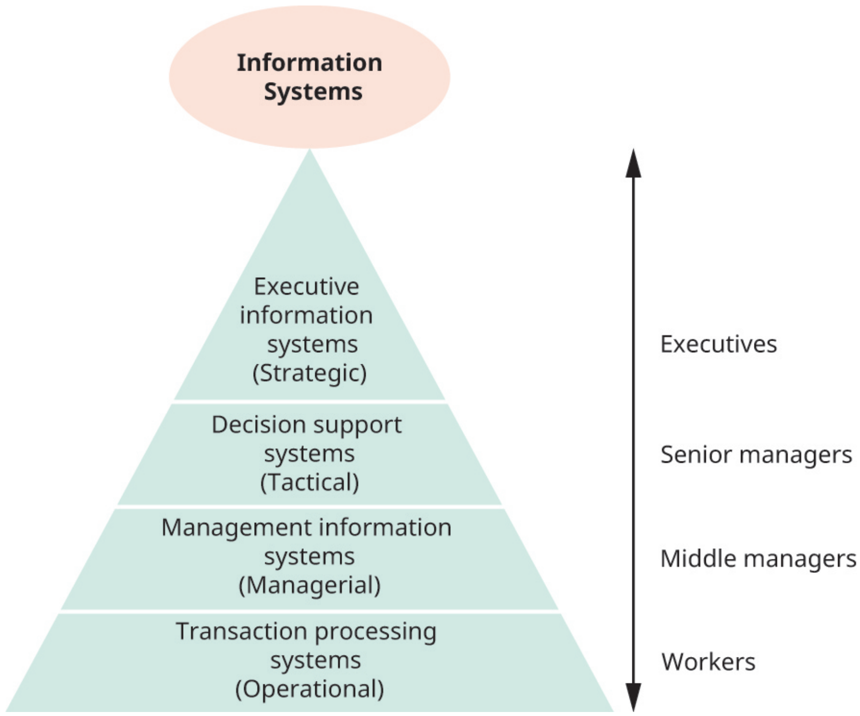


Figure 1.3 Information systems include several types of systems with distinct purposes. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Let us take a closer look at each type of information system and explore their purposes.

- An **executive information system (EIS)** supports the strategic information needs of top executives, providing the information needed to handle executive functions, such as developing an organization's strategic goals and objectives and plans for achieving them. This includes providing the information needed for managers to understand and manage their organization's supply chain and value chain, which can be helpful to streamline production processes and provide better customer service. Supply chain management is an example of how an EIS can be used as an interorganizational information system, which occurs when two or more organizations use IS to conduct business electronically.
- A **decision support system (DSS)** assists in decision-making by providing interactive tools and access to data analysis. Typically, senior managers use a DSS to obtain tactical information that helps them make routine, short-term decisions about an organization's operations. This helps ensure that organizations stay on track to achieve long-term goals and objectives. Interactive tools available through a DSS enhance these efforts by providing information and technology needed for activities such as project management and employee training.
- A **management information system (MIS)** provides middle managers with reports and summaries to support decision-making and managerial functions. For example, middle managers may use an MIS to generate reports, such as budgeting documents and cash flow statements, to understand an

organization's financial status. In many organizations, this type of system provides the data for an organization's balanced scorecard (BSC), which is a performance metric used by strategic managers to identify an organization's various functions and monitor outcomes. By providing the data necessary for the BSC, an organization's MIS function provides invaluable support.

- A **transaction processing system (TPS)** handles day-to-day transactions, such as order processing and payroll. For frontline staff, a TPS provides information necessary to handle an organization's daily operations, such as inventory reports and customer service records.

In addition to these four types of information systems, an **enterprise resource planning (ERP) system** is a software system that helps an organization manage various types of information systems within the organization, and integrate business processes and functions across the organization. For example, large organizations may rely on an ERP system to handle human resource management throughout the organization. An ERP is also a useful tool for functions such as project management, accounting and financial management including payroll, and tracking customer service.

Application of Information Systems in Business

Think about a visit to a coffee shop, from ordering to receiving the order, through the lens of IS. First, think about how a barista takes an order at the register. That's the point-of-sale (POS) system at work. The POS system is an information system that streamlines transactions, helping businesses track sales, manage inventory, and even understand customer preferences when tracked with tools such as customer loyalty cards. When a customer switches from their regular black coffee to a caramel macchiato, the system takes note and updates their preferences, contributing to a personalized customer experience.

Now, imagine if the coffee shop had no system to track sales, manage its supplies, and keep track of customer preferences. What do you think might be some of the challenges a business would face if they did not have a way to gather, track, and analyze this data? This is where ERP systems come into play. ERP systems integrate various business processes, ensuring that everything from bean procurement to milk deliveries is synchronized. This not only prevents the coffee shop from running out of their most popular blend, but also helps them manage costs and operate more efficiently.

The POS and ERP systems are not the only information systems in a coffee shop. Most coffee shops have Wi-Fi, which is another information system that includes hardware, software, and the networks that connect them. The coffee shop's Wi-Fi is a small-scale example of how businesses use IS to stay ahead of the competition, whether it be locally, nationally, or globally.

In essence, information systems are about more than simply computers and gadgets. They are the invisible architects that shape our daily experiences, whether we're grabbing a coffee or navigating the complexities of a global market.

CAREERS IN IS

Careers in IS

Students who are interested in the field of IS have a variety of career options. There are technical jobs that require in-depth knowledge of computers, such as software developers who design, create, and test the software applications necessary to develop and maintain an information system. Cloud computing engineers also fall into this category, and they must have the skills to guide and support organizations as they connect their systems to the cloud and use it to conduct business.

But not all IS jobs are technical. Students who find the field intriguing but want a less technical job also have career options. For example, systems analysts explore an organization's operations to identify areas where technology can be used to help an organization be more efficient and cost-effective. Information systems managers oversee how information systems are planned, implemented, and maintained to ensure that the functionality aligns with their organization's goals and objectives.

The Historical Evolution of Information Systems

The basic purpose of information systems—processing and sharing information—has been part of our communication practices since the beginning of civilization, evolving from simple cave drawings to the complex technology we have today. Understanding the background and history of IS helps us appreciate the importance of IS, how it has helped shaped civilizations across the ages, and why it continues to be a vital part of our lives, both personally and professionally.

Evolution of Communication and Information Sharing

The earliest forms of communication evolved from body language, hand signals, and drawings to spoken and written languages. As written language developed around the world, various societies invented ways to print written works that could be shared with others. These earlier means of communication provided essential information without technology components like those we think of today, such as database management systems, data networks, hardware, and software.

For hundreds of years leading up to the twentieth century, early technology laid the foundation for today's complex information systems. The printing press was the dominant invention that promoted communication and information sharing for centuries before the inventions of the telegraph and the telephone. By the end of the 1800s, the basic design of the telephone, which is still the foundation for today's landline handsets and cell phones, was in place. The telephone revolutionized communication, allowing real-time conversations for sharing information for both personal and business purposes.

The telephone took another step forward in 1973 when Martin Cooper, an engineer for Motorola, made the first call on a wireless cellular telephone. This launched a revolution as cell phones progressed to eventually become a vital personal resource for individuals around the world. By January 2024, Pew Research Center found that 97 percent of adults in the U.S. owned a cell phone.[2]

As this information shows, communication has been paramount for humans since the beginning of civilization, and we have strived to find more and better ways to stay connected with one another.

Development of the Internet

The inventions of the computer and the internet have been instrumental in the development of some of the technology necessary for today's information systems. While societies developed a variety of methods for communication, they also created tools for calculations, establishing the foundation for modern computers. The abacus, which can be traced to at least 1100 BCE, is the oldest known calculating tool. Analog and digital calculators were invented in the 1600s, followed by the Jacquard loom in the early 1800s. The first modern analog computer was developed in 1930, and in the 1940s, IBM produced fully functional computers that evolved over the decades to the laptops and other computers that we have today.

Initially, computers were not linked by data networks and could not be used as communication tools. Rather, their primary purpose was to calculate, process, and store information. For example, the U.S. government used early computers to compile and calculate statistical data gathered from census questionnaires. Businesses first used computers for purposes such as tabulating and storing financial information, and academic institutions relied on these basic computers to organize and analyze research data.

The inventions of the telegraph and telephone laid the foundation for the 1969 introduction of the U.S. Advanced Research Projects Agency Network (ARPANET). This network linked computers to one another and

2 "Mobile Fact Sheet," Pew Research Center, November 13, 2024, https://www.pewresearch.org/internet/fact-sheet/mobile/

became the forerunner to the internet. Focused on the military and universities, which needed the ability to collaborate and connect project team members in multiple locations, the ARPANET provided a means for professionals in separate locations to share information and computing resources. Using satellite links and packet-switching technology, which transfers data in small pieces as it is routed through a system, computers in the network could communicate with each other. As technology progressed, the ARPANET developed features such as the following:

- telnet, which enables users on one computer to log into other computers using the same network
- FTP protocols, which allow electronic file transfers
- list servers, which send a single message to multiple subscribers
- routers, which handle data packets

Figure 1.4 shows the expanse of the network in 1974.

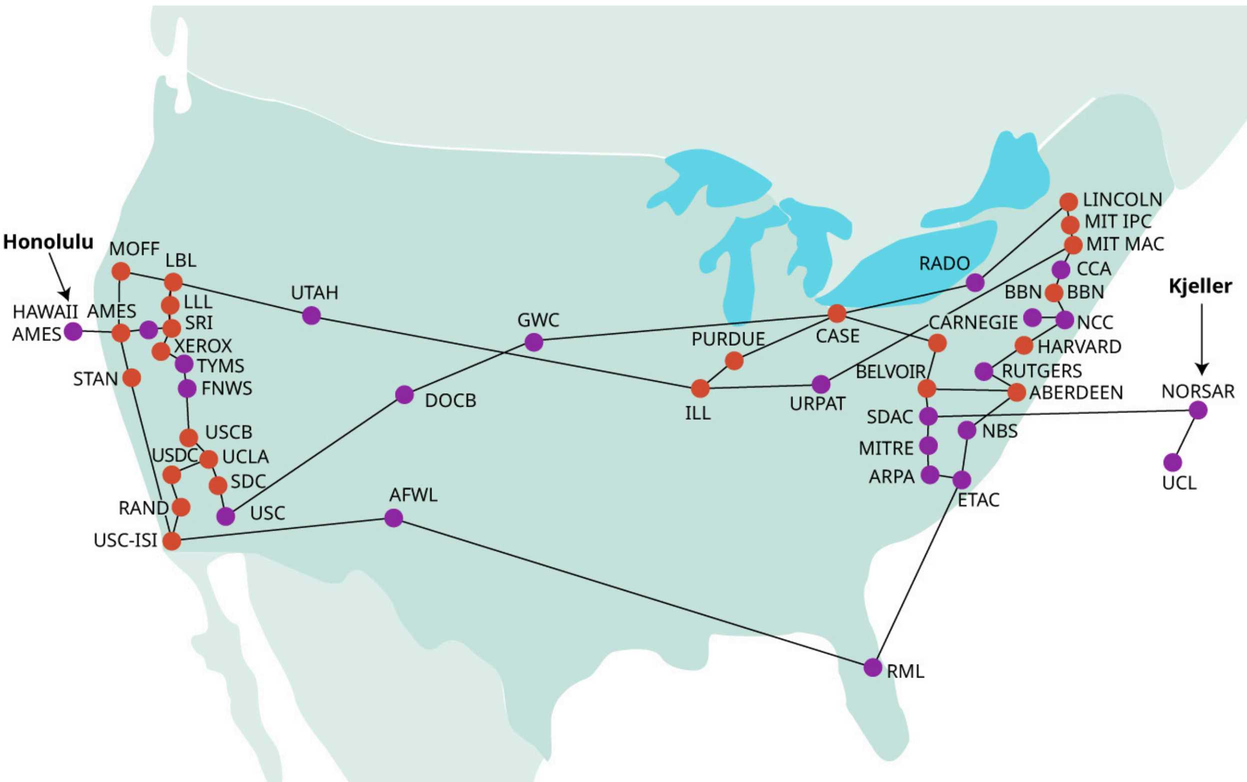


Figure 1.4 In the 1970s, the Advanced Research Projects Agency's network consisted of a series of nodes (connectors) and lines that stretched across the continental United States. (credit: modification of work "Arpanet 1974" by "Yngvar"/Wikimedia Commons, Public Domain)

During the 1970s, scientists Vinton Cerf and Robert Kahn developed the communications model for Transmission Control Protocol/Internet Protocol (TCP/IP). This established the standards for transmitting data among multiple networks of computers. In 1983, ARPANET adopted TCP/IP, providing the framework for researchers to create the vast network that evolved into today's internet.

In 1990, computer scientist Tim Berners-Lee advanced this technology when he invented the World Wide Web, providing users with the ability to access online information through websites and hyperlinks. The internet has made global communication and information sharing commonplace and convenient for anyone with computer access.

As this history shows, the goal of information technology has been to find ways to do things more efficiently, saving time while increasing productivity. The technological advancements in computer science and information technology have provided the additional technology and frameworks needed to develop today's robust information systems.

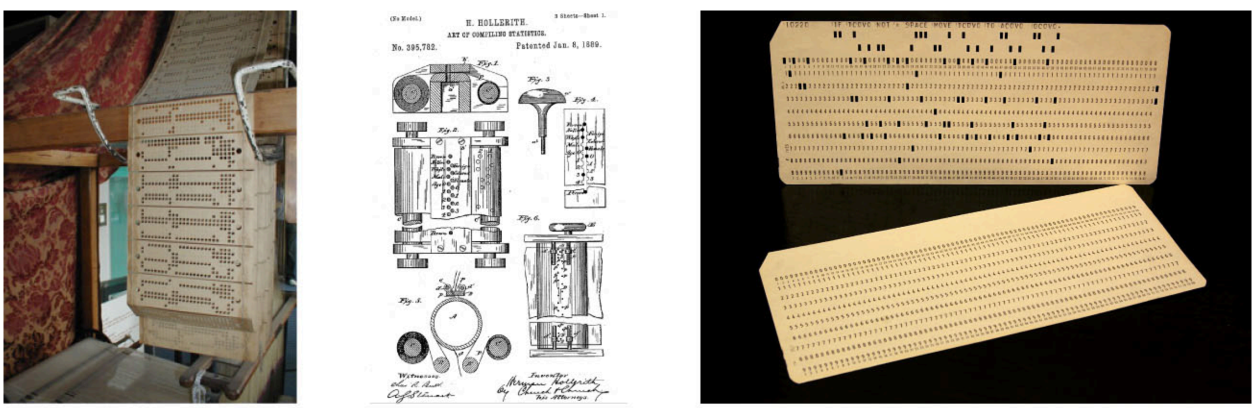
LINK TO LEARNING

Watch this video for a [synopsis of the history of the internet (https://openstax.org/r/109HistInternet)](https://openstax.org/r/109HistInternet) provided by NBC News. It offers perspective on the roots of our current information systems and sets the stage for future trends in information systems that seem to be evolving at an exponentially faster pace.

Evolution of Computer Hardware and Software

While technology evolved and the internet was launched, computer hardware and software also evolved. Hardware includes the tangible parts of a computer, such as the motherboard, hard disk drive, and central processing unit, as well as accessories such as electrical cords, keyboards, and monitors. Software refers to the programs and instructions that make computers functional, able to follow commands and carry out tasks. Common examples of software include word processing and spreadsheet programs.

To understand how computers developed, consider the Jacquard loom. This 1801 invention helped artists weave cloth. The loom was used to produce patterned cloth, and by using punched pasteboard cards, Jacquard applied binary code to the weaving process, revolutionizing the way fabric was created. The loom itself was constructed of metal and wood, which functioned as the machine's hardware. The rods in the loom were controlled by pasteboard cards that were stiff and included holes to instruct the rods in the steps needed to weave a specific pattern of cloth (Figure 1.5). The design of the loom helped early computer designers understand the concepts and importance of computer hardware and software by applying binary code.



(a) (b) (c)

Figure 1.5 (a) Jacquard's loom, which performed calculations using a punch card system, was an early development in computing, as was (b) Herman Hollerith's punch-card tabulating machine, for which he was awarded a patent in 1889. (c) Each hole in a punch card equals a piece of data (called a "bit" today) that the machines read. (credit a: modification of work "Jacquard.loom.cards" by George H. Williams/Wikimedia Commons, Public Domain; credit b: modification of work "Holerith395782Figures1-6" by Herman Hollerith/ Wikimedia Commons, Public Domain; credit c: modification of work "2punchCards" by José Antonio González Nieto/Wikimedia Commons, CC BY 3.0)

While the cards' pasteboard was hardware, the patterns of holes in the cards were software because they provided instructions and determined which patterns would appear in each piece of cloth produced by the loom. This process demonstrated how hardware and software could be coordinated to achieve specific tasks, providing an important framework as computers were developed.

LINK TO LEARNING

Early computers were large and bulky, with some filling entire rooms. Personal computers became available during the 1970s, and in the early 1990s, laptop computers were introduced, followed by the Palm Pilot and cell phones with built-in cameras. To learn more, you can browse photos of many early computers (https://openstax.org/r/109EarlyComps) and explore the evolution of computer hardware and software.

Digital Media and Its Impact on Human Communication

As computers have evolved to become more powerful and offer more features, information sharing experienced the next wave of major advancement through digital media. The term **digital media** refers to the content developed, stored, and distributed via mobile devices—such as news stories, blogs, videos, and online games—as well as the hardware—flash drives, DVDs, and digital computers—used to store and share this media. Digital media falls into one of six categories: audio, video, social media, advertising, news, and literature.

The impact of digital media is transformative, as it promotes information sharing, enabling people, businesses, and societies around the world to communicate. With digital media, which has included faster network speed and more robust architecture, students can take classes online; organizations can conduct business worldwide; news outlets can research, write, and distribute stories globally; and people can conduct real-time conversations with coworkers, friends, and families around the world. We use digital media to learn, be entertained, and conduct transactions such as ordering takeout food from a local restaurant or streaming a movie. The evolution of digital computers has caused a major disruption to media and publishing industries that create print newspapers, magazines, and books, now that television programming and advertisements are available online twenty-four hours a day, seven days a week.

As the internet developed, users were able to use computers to share information through resources such as emails and online access to news sites. By the late 1970s, online text-based games became popular, and many organizations began using computers to operate online public bulletin boards. Later, files could be uploaded and shared, and by the late 1990s, it was possible to post and share music and videos online. These technological advancements were important to support the evolution of information systems, giving users more options for communication and information sharing.

Web 2.0 and Social Media Platforms

The initial version of the internet is known as Web 1.0, and it featured websites that were static, which means that users could read website content but could not interact with it. Shortly before the beginning of the twenty-first century came the next generation of the internet. Known as Web 2.0, the basic functioning of the internet changed to enable, and even encourage, users to be active participants on the internet by contributing content, such as comments, blogs, photographs, and videos.

No technological improvements or advancements were necessary to move from Web 1.0 to Web 2.0. Rather, this transition was simply a change in the way the internet was perceived and used. This led to the launching of applications and websites that led to the growth of social media. Any type of electronic communication tool that enables users to establish online communities where they share content, including personal messages, ideas, photographs, and videos is considered **social media**.

Once technology was available to support social media, many new websites were developed. For example, Wikipedia was launched in 2001, providing users with an online encyclopedia that enables information sharing on any topic. Facebook started in 2004 as a way to connect students at Harvard University and later evolved into the social networking service of today that provides users throughout the world with a means to communicate, connect, and share information. In February 2005, YouTube's online platform to share videos was launched. A few months later, in June 2005, Reddit began, providing users with a means to upload a variety of content—including images, videos, and text posts—that other users could vote up or down. In 2010, Instagram launched, offering a social networking service to share photos and videos. In 2016, China launched TikTok, a social media platform for sharing videos.

The concept of social media, the process of social networking via technology, can be traced back to the telegraph. With the ability to transmit messages electronically over many miles, the telegraph gave people a means to interact socially without being face-to-face. Later, when the ARPANET began, email became a popular form of social media. As the world began to appreciate the convenience and benefits of interacting online, Web 1.0 became Web 2.0. To understand the impact of Web 2.0, consider that by early 2024, 5.04 billion people (62.3 percent of the world's population) were using social media to communicate and share information.[3]

Future Trends in Information Systems

Our world is complex, and information helps us make sense of the people, places, things, and events that surround us. Through information systems, we can communicate and share information to learn from each other, solve challenging problems, and explore new opportunities to meet our needs, both personally and professionally.

To ensure that people can continue to communicate and manage the complexities of the world, information systems, including processes to share information, continue to evolve. Emerging technologies, such as artificial intelligence (AI), machine learning (ML), and blockchain, have the potential to provide many benefits to much of the world's population, but can also raise or expand ethical concerns. As these systems continue to advance, we will need to balance these ethical concerns with the benefits they bring.

Features of Information Systems

As you have learned, the components of information systems are people, hardware, software, data, and procedures. These components work with the elements of information systems—input, processing, output, and feedback—and the operations of these systems and the processes to manage data and ultimately to support business operations.

Components of Information Systems

The components of information systems all interact closely to make the system function. People are a vital part of information systems, both as developers and as system users. An important aspect of systems development is ensuring that a system is user-friendly. To maximize functionality and promote information sharing, systems must be accessible to individuals without a background in technology.

Hardware provides the necessary foundation and tools that make software operational, and software is necessary to process and store data. In addition to enabling software, hardware such as keyboards and mice provides users with the means to access the system for the purposes of inputting and retrieving data. Without software, the hardware does not have the instructions needed to function appropriately and perform specific tasks. Two types of software—operating systems and applications—are necessary for information systems to function. The **operating system (OS)** functions as a computer's manager by operating the computer's memory and other hardware resources such as disk storage. Additionally, the OS provides the interface for users to work with the computer, and it manages the computer's application software programs. Examples of an OS include Linux, which is open source, and Microsoft Windows, for which a license must be purchased.

Programs that enable computers to perform specific tasks are called **application software**. Examples of application software include word processing and spreadsheet programs, as well as web browsers and presentation software. The mobile applications on your mobile phone that enable you to do things like send texts and play games are also examples of application software.

Once hardware and software are in place, the next essential component is data. As noted earlier, the basic concept and purpose of information systems is processing and sharing information, and data are necessary to achieve this objective. This information may include both quantitative and qualitative data. Numerical information is called **quantitative data**. In IS, this may include statistics, financial information, and other data

3 "Overview of Social Media Use," *Digital 2024: Global Overview Report*, Kepios, January 2024, https://datareportal.com/reports/digital-2024-global-overview-report.

such as marketing trends that are expressed numerically. Nonnumerical information is called **qualitative data**. Depending on the needs of the system, information may include a variety of qualitative data, such as customer names and addresses, photographs, videos, descriptive information, individual opinions, and any other nonnumerical information needed to meet the system objectives.

Once a system has hardware, software, and data, procedures are essential to ensure that it functions appropriately. These procedures should be written in detail to provide instructions and policies for the use of the system. These procedures should include information about security, such as who has authorization to use the system and policies for maintaining and updating passwords.

Elements of Information Systems

Once the components are in place, several elements are necessary for the information system to function. These elements include environment, input, processing, output, control, and feedback.

- Factors such as physical location and network capabilities that affect a system and help determine how it operates are referred to as its **environment**. This also involves the purpose and context of a system, including whether the majority of users are tech savvy or have limited skills in technology. To ensure that a system is set up appropriately, it must be implemented in an environment that will promote its capabilities and meet the goals and objectives. For example, if an information system contains sensitive information that must be protected from unauthorized users, the physical location of the system must be in a secure building, and the system itself must include cybersecurity features that guard against hacking and other unauthorized use.
- The **input** is the data that are collected and entered into the system by users or automatically when transactions occur, such as when you make a purchase with a debit card and your checking account is automatically charged for the purchase. An information system must include the software needed to handle the types of data required for the system. For example, a system that handles financial data needs spreadsheets, and a system that handles qualitative data such as reports needs word processing capabilities. Typically, an information system needs multiple software applications to handle the diverse types of data required for the system.
- The performance of tasks in order to make data useful in a system is known as **processing**. For example, once financial data are entered into a spreadsheet, that data must be computed in order to yield useful information such as the costs to produce goods and services, the number of sales per month, and the profits earned per quarter. The calculations to derive this data are tasks performed as part of processing.
- The data and information that a system generates and provides to users is called the **output**. Data about a business's costs, sales, and profits are examples of information system outputs. Information system users must be able to retrieve this output in a secure and user-friendly manner whenever data are needed.
- A policy or procedure that ensures a system functions effectively, efficiently, and securely is called a **control**. Controls typically fall into two categories—application and general.
    - An **application control** is built into the system and includes features such as firewalls, encryption, and access control.
    - A **general control** refers to a process that outlines how an information system is to be used and includes requirements such as routine password updates.
- Information that users provide to managers about an information system's functionality is called **feedback**. When users report problems with the system or note a procedure that can be improved, this feedback is used to modify and improve the functionality of the information system.

Operations of Information Systems

Information systems operations refer to how the system is used. This includes data capture, processing, storage, retrieval, and dissemination.

- The process of gathering data from various sources such as customers and financial records, and inputting this data into the system is called **data capture**.

- Using calculations, manipulations, and analysis to transform data into useful information is called **data processing**. This includes, for example, the processes of adding the number of products sold during a month and calculating the profits earned from these sales.
- The process of maintaining a system's data and information in a location that is secure, reliable, and accessible to authorized users is called **data storage**. Location refers to the specific computer hardware and software used for an information system. These must include the tools and capability to store and manage data, such as databases. Location also refers to the physical building that houses the computer hardware and software for the system. This location must be secure, protecting the computer hardware and software from unauthorized users, as well as environmental threats such as earthquakes, fires, and floods.
- The process of retrieving data from storage is called data retrieval. For example, users should be able to load and review applications, such as spreadsheets, that store data. Users should be able to download this information and use it for authorized purposes, such as research and preparing reports.
- The process of distributing and sharing information such as reports, videos, photographs, and other system outputs to users is called **data dissemination**.

Impact on an Organization's Operations

Organizations have come to rely on information systems as a critical resource. A well-developed and maintained system offers important benefits to organizations of all types, including businesses, government agencies, and nonprofit associations. Information systems bring interconnectedness to an organization and provide many benefits, such as improved efficiency, more robust decision-making, enhanced communication processes, increased productivity, and competitive advantages.

Information systems improve efficiency by reducing the time, effort, and costs required to perform tasks and conduct transactional business, which may include processes such as inventory management, filling orders, billing, payment processing, shipping, and returns and refunds. Information systems can make certain tasks easier to perform and can automate others. They can also improve accuracy, making an organization's data more reliable.

To understand how information systems improve an organization's transactional business, consider a food order through a delivery service. The customer places an order online, the restaurant's system processes it, and the app collects the payment. Generally, this process is simple and convenient for the customer and the restaurant. Because the customer entered the order online, the restaurant knows exactly what food they want, which should reduce the chance for errors in the order. Later, the customer can use the system to let the restaurant know about any concerns or to provide a positive review. By using information systems, restaurants and delivery services across the nation have streamlined the process of taking and filling takeout delivery orders, improving customer service while creating a better system of recordkeeping.

Information systems help organizations gather reliable data and make better decisions by providing timely information and the option of developing scenarios, using data in mock situations to examine potential problems or opportunities. The decision-making processes that have been improved by information systems include performance evaluations, risk assessment, budgeting, cost analysis, forecasting, resource allocation, strategic planning, investment analysis, and competitive analysis.

Information systems improve organizational communication by making it easier for colleagues and teams to share information and collaborate. This collaboration is enhanced because these systems enable organizations to work with better and more accurate data. Collaborative business processes positively impacted by information systems include group decision-making, conflict resolution, relationship management, and negotiation.

Consider a team of colleagues who are working together to develop a marketing plan for a new product. By using information systems, each member of the team can access and share data about the product to understand its purpose, target market, and options for marketing. By accessing data on the organization's previous marketing efforts, they can understand and share information about marketing techniques that have worked well for the organization in the past, as well as those that were not as effective. The information system provides the team with the data and tools they need to fully understand the product and the marketing goals, and gives the team the resources they need to communicate and negotiate to develop a successful marketing plan.

An information system also increases an organization's productivity by enabling users to automate certain tasks and complete others quickly. They streamline workflows, enabling organizations to develop and adhere to workflow processes that are more efficient, thus reducing errors and waste, such as discarded paper.

These improvements generally result in reduced organizational costs and improved quality of an organization's operations, including the goods and services produced. Information systems enable organizations to provide better customer service, which typically leads to more satisfied customers, increasing the likelihood that customers will rely on the organization again when they need its goods or services.

LINK TO LEARNING

By now, you should understand that information systems are a vital tool for organizational success. To learn more, explore how nineteen companies, including Lego and Sephora, are using information systems (https://openstax.org/r/109ISinWorkplce) in their operations. As you read their stories, consider how the field of IS improved operations, whether these companies could have accomplished their goals without IS, and whether you would recommend these companies use IS in the future.

1.2 Frameworks of Knowledge and Industry Standards

Learning Objectives

By the end of this section, you will be able to:

- Discuss the use of frameworks and industry standards in IS
- Identify the frameworks and standards in IS
- Correlate the frameworks and standards to knowledge as an IS professional
- Discuss characteristics and roles of IS professionals

To promote best practices and help organizations achieve information systems goals and objectives, the field of information systems (IS) is guided by frameworks and industry standards. A **framework** refers to a tangible structured set of guidelines and best practices that is used to guide the process of developing, implementing, managing, or maintaining a business process, policy, system, or procedure --such as an information system. An **industry standard** is a policy, procedure, or requirement widely used and supported in an industry to promote efficiency and quality in goods and services.

Frameworks and industry standards can help IS professionals develop and maintain robust systems that enable organizations to function effectively and competitively. In addition, a framework can enable an information system to function in everyday life. For example, a fitness app can help you set fitness goals, establish an exercise plan, and track food and nutrient intake. It may provide access to free information and suggestions from athletes, fitness trainers, and experts in wellness. Similarly, an organization can use information systems to support decision-making and set goals for any function, including financial management, human resources, and marketing. Once an organization establishes its goals, it can use information systems to develop a plan of action to achieve those goals and then use it to carry out their plans, track progress, and achieve success in the marketplace.

Use of Frameworks and Industry Standards in Information Systems

When developing an information system, frameworks provide guidance to help IS professionals apply critical thinking as they identify the goals of the system and problems that can be resolved by the system. Frameworks promote proactive communication and help IS professionals organize their ideas and provide a foundation for strategic planning to develop and maintain a system that meets an organization's specific needs. As part of this process, frameworks also provide IS professionals with resources such as continuing education, best practices, and guidelines for systems operations.

Industry standards help IS professionals ensure that the system they develop has the appropriate infrastructure and technological components required to function efficiently. This includes ensuring the system is compatible with information systems used in other organizations. After all, an important objective of IS to enable information sharing internally and externally as organizations interact in the marketplace.

Specific Frameworks and Standards in Information Systems

Starting with the most commonly used frameworks, those applicable to IS include Agile, Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), the Skills Framework for the Information Age (SFIA), Waterfall, and Zachman.

Agile methodology is a framework used to guide project management, primarily by dividing projects into phases, or sprints. Typically, these sprints include planning, designing, developing, testing, deploying, and reviewing. After each sprint, the project team examines their progress and adjusts before moving to the next sprint. Agile can be a useful framework as IS professionals plan and develop an information system. Several versions of Agile frameworks are used for project management, including Kanban, Lean, and Scrum.

Control Objectives for Information and Related Technologies (COBIT) is a framework that develops and maintains an information system using five processes: Evaluate, Direct, and Monitor (EDM); Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA) (Figure 1.6). COBIT is promoted by the Information Systems Audit and Control Association (ISACA), which is a global organization that provides training, research information, news updates, advocacy, and related support for IS professionals and others involved in information technology.

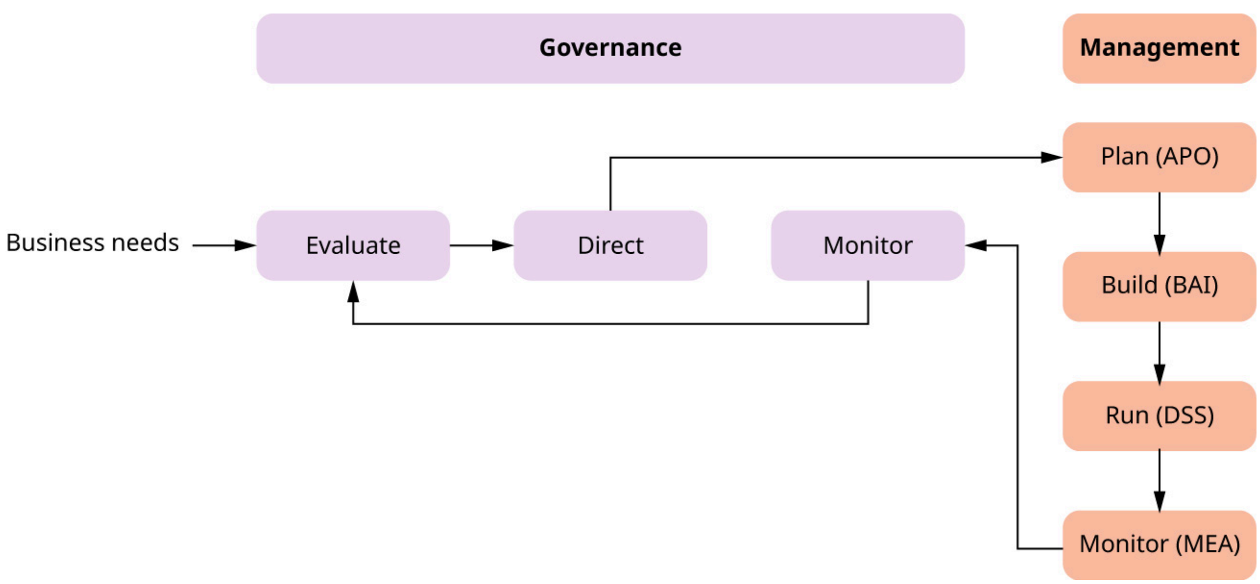


Figure 1.6 COBIT's framework provides IS professionals with five processes—Evaluate, Direct, and Monitor (EDM); Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA)—that can help develop and maintain an information system. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Information Technology Infrastructure Library (ITIL) is a comprehensive framework of documentation that discusses best practices for managing information technology. ITIL is managed and updated by AXELOS, a company that provides training and certifications to various technology professionals, including those in IS. ITIL offers guidance, as well as professional certification, for carrying out twenty-six processes in the areas of service strategy, design, transition, operation, and improvement.

The **McKinsey 7-S Framework** focuses on how an organization can be efficient and effective with interaction and coordination of its staff, structure, strategy, skills, systems, style, and shared values. The goal of the framework is to determine how an organization can be effective with interaction and coordination of the seven elements:

- Staff: the people who lead and work in an organization, as well as the tools to support the staff, including training and incentive programs
- Structure: how an organization is designed, including its hierarchy and chain of command
- Strategy: the organization's goals/objectives and the plans to achieve these
- Skills: the skills, knowledge, and competencies held by the organization's staff
- Systems: the workflow processes used to achieve the organization's goals and objectives
- Style: the tone at the executive level established by the organization's leaders and managers
- Shared values: the organization's mission and values that motivate its operations

LINK TO LEARNING

The McKinsey 7-S Framework was introduced in the 1970s to emphasize the importance of coordination within an organization across its structure. Review this interactive presentation about the framework's applicability today (https://openstax.org/r/109McKinsey) from McKinsey and Company.

The McKinsey 7-S Framework can be used by following four steps:

1. Identify the parts of the organization that are not aligned with shared values, including a shared mission, goals, and objectives.
2. Determine the design and structure that will enable the organization to achieve alignment and reach its goals and objectives.
3. Identify areas where changes are needed to update the organizational design.
4. Implement the necessary changes.

This framework can help ensure organizations are in alignment and have an effective design, making it easier to develop and maintain the appropriate information systems to meet the organization's needs.

The **Skills Framework for the Information Age (SFIA)** provides a comprehensive skills and competency framework in a common language for the IT industry. It includes the steps listed in Figure 1.7. It was developed and is overseen by the SFIA Foundation, a global organization committed to helping IS and other technology professionals acquire the skills and competencies needed to successfully develop and manage technology. Organizations around the world in both the public and private sectors use SFIA to map out the knowledge and expertise needed to fill each role in their organizations. This includes entry-level to advanced positions in the areas of technology development, strategy, architecture, and support.

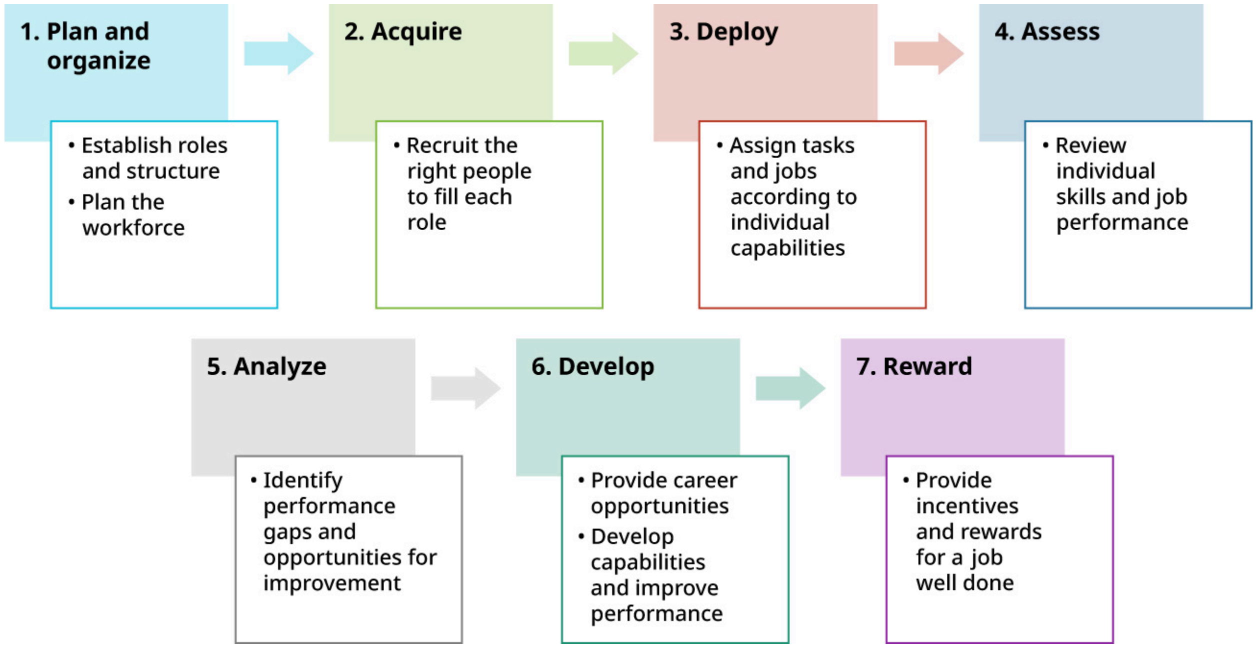


Figure 1.7 SFIA can be an important framework as organizations develop the skills needed to manage technology. This includes planning and organizing, acquisition, deployment, assessment, analysis, and development. It is also important that organizations reward employees and recognize their success. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Individually, IS professionals use SFIA to identify the skills they personally need to develop to perform their jobs and advance their careers. SFIA is structured to help organizations and individuals achieve success in the following seven levels of responsibility:

- Level 1, Follow: This level applies to entry-level positions that are closely supervised, perform routine tasks, rely on basic tools, and have minimal influence on the work environment, essentially following others as they perform their jobs.
- Level 2, Assist: These employees also work under close supervision, but their work is a bit more complex, and they have more influence with colleagues.
- Level 3, Apply: At this level, employees receive more general supervision, and they have more autonomy. Their work is more complex and may not be routine. They also may be allowed to make some decisions on their own and may oversee other employees.
- Level 4, Enable: Employees at this level have much more complex work in a broader range of contexts. While they receive general direction, they have considerable autonomy, as well as personal responsibility for work outcomes.
- Level 5, Ensure and Advise: At this level, employees receive broad direction, giving them more autonomy, including the ability to self-initiate work that they think should be performed. Their tasks tend to be complex and are an integral part of an organization's strategic plans.
- Level 6, Initiate and Influence: Employees who initiate and influence play a central role in establishing an organization's objectives and assigning responsibilities to subordinates. These employees perform highly complex tasks and make decisions that directly impact an organization's performance and achievement of organizational goals and objectives.
- Level 7, Set Strategy, Inspire, and Mobilize: The final and highest level is filled by an organization's top leaders and managers. These individuals establish an organization's policy objectives and have oversight and accountability for all decisions made and actions taken throughout the organization.

SFIA is an important framework used globally to promote success in the digital world. Its common language helps technology professionals across the globe integrate the processes they must learn to successfully manage technology.

Waterfall is a structured, linear framework used to guide project management. Generally, the steps of

Waterfall include compiling documentation of the project requirements, using logical design to brainstorm how to approach the project, developing the physical design, implementing the design plan, verifying and testing the design, and maintaining the design once it is in use. While Waterfall tends to focus on computer programming and coding, the framework can be applied to IS.

The **Zachman Framework** provides a structure for developing and organizing the artifacts of enterprise architecture, including data and documents, which are vital for a robust information system. Using a 6 × 6 matrix, the Zachman Framework asks the following six questions to identify the needs and perspectives of stakeholders in a particular system:

- *What?* seeks to understand the data needed for the system by learning about the organization's data, objects, and information.
- *How?* seeks to understand the organization's processes and functions.
- *Where?* seeks to learn where the organization operates.
- *Who?* seeks to learn who the organizational members are, as well as gather details about the organization's units and hierarchy.
- *When?* seeks to learn the organization's schedule of operations, including when processes are performed.
- *Why?* seeks to learn why the organization has selected certain systems and solutions for its enterprise risk management and information systems. This question also seeks to determine what motivates the organization to perform certain functions.

As shown in Figure 1.8, these questions are posed across the top of Zachman's 6 × 6 matrix. On the left side of the matrix, the rows list the organization's stakeholders. To understand the system needs, the stakeholders' perspectives are entered into the appropriate cells in the matrix. The Zachman Framework can be an important tool to understand what an organization's information systems should entail and develop the appropriate enterprise architecture to support that system.

	What (Data)	**How (Function)**	**When (Time)**	**Who (People)**	**Where (Location)**	**Why (Motivation)**
Scope (Contextual)	List of things	List of processes	List of events	List of organizations	List of locations	List of goals
Enterprise Model (Conceptual)	Semantic model	Business process model	Master schedule	Work flow model	Logistics network	Business plan
System Model (Logical)	Logical data model	Application architecture	Processing structure	Human interface architecture	Distributed system architecture	Business rule model
Technology Model (Physical)	Physical data model	System design	Control structure	Presentation architecture	Technology architecture	Rule design
Implementation (Detail)	Data definition	Programs	Timing definition	Security architecture	Network architecture	Rule specification
Functioning Enterprise	Usable data	Working function	Usable network	Functioning organization	Implemented schedule	Working strategy

Figure 1.8 The Zachman Framework provides a structure for developing and organizing the artifacts of enterprise architecture. By asking *what*, *how*, *where*, *who*, *when*, and *why*, the Zachman Framework can help IS developers understand an organization's needs from the perspective of an organization's various stakeholders, including executives, managers, and technicians. (credit: modification

of work "Zachman Framework (9026775815)" by National Institute of Standards and Technology/Wikimedia Commons, Public Domain)

The industry standards that are applicable in IS include the American Society for Industrial Security (ASIS), the Federal Information Security Modernization Act (FISMA), IS2020, ISO/IEC 27001, and the Open Group Architecture Framework (TOGAF).

The **American Society for Industrial Security (ASIS)** is a global organization that provides training and certification to help professionals in all industries provide security for people, property, and information. ASIS is a global organization that collaborates with public and private organizations throughout the world—such as the Department of Homeland Security and the Federal Bureau of Investigation—to ensure that IS professionals and others involved in security have the resources needed to successfully handle security issues at every stage of their career.

IS professionals who work for government agencies or private businesses that contract with the government should be familiar with the **Federal Information Security Modernization Act (FISMA)**, which sets the guidelines and standards for security that affected organizations are required to meet to minimize the possibility that data will be stolen, lost, or misused. Under FISMA, affected organizations must have a security strategy that addresses issues such as system access control, risk assessment and management, information integrity, audit and accountability, incident response, and staff's continuing education.

IS2020 is a competency model that provides guidance and standards to higher education institutions to ensure that undergraduate IS programs effectively prepare students for careers in IS. Developed by an international task force of members of the Association for Computing Machinery (ACM) and Association for Information Systems (AIS), IS2020 outlines the curriculum that should be offered to IS students and the competencies that students should develop as they complete the curriculum. This includes the knowledge, skills, and dispositions that students need for successful careers in IS, as well as the tasks that students should learn to perform.

ISO/IEC 27001 is a worldwide standard established by the International Organization for Standardization that defines the requirements information systems must satisfy to provide adequate security for any system. ISO/IEC 27001 applies to all sizes and types of organizations in both the public and private sectors. The standard focuses on cybercrime but helps organizations guard against any threats to data availability, integrity, and confidentiality.

The Open Group Architecture Framework (TOGAF) is a trademarked standard in its tenth edition that promotes best practices for IS and other technology. TOGAF is used by organizations throughout the world in both the public and private sectors to support requirements management for enterprise architecture. The areas covered by TOGAF include architecture vision, business architecture, information systems architectures, technology architecture opportunities and solutions, migration planning, implementation governance, and architecture change management.

LINK TO LEARNING

The Open Group Architecture Framework (TOGAF) contains vision, requirements, business architecture, information systems architecture, technology, and architecture realization. TOGAF can be an important standard to support organizations as they develop and manage the requirements for enterprise architecture. As their Architecture Development Method (https://openstax.org/r/109ArchDevMethd) shows, TOGAF covers all aspects of enterprise architecture, including information systems. This framework provides an essential structure for managing and aligning strategies with business goals.

Application of the Frameworks and Standards

IS professionals should rely on the frameworks and standards applicable to their organization and specific role to guide their work. This helps ensure that the work meets the organization's needs, while also following standards important for maintaining IS compatibility with other organizations.

It is also beneficial to join one or more professional organizations such as the Association for Information Systems (https://aisnet.org/), International Association for Computer Information Systems (https://www.iacis.org/), or Information Systems Audit and Control Association (https://www.isaca.org/). Such organizations provide members with important resources, including training, as well as news and updates about events and changes important to IS professionals. Joining such organizations and taking advantage of learning opportunities helps ensure that you obtain the appropriate continuing education to stay abreast of changes and new requirements in the field of IS. In addition, members of such organizations gain access to colleagues around the world who can become an important networking resource for information sharing and collaboration.

GLOBAL CONNECTIONS

A Symbiotic Relationship: IS and Globalization

Information systems have allowed companies to increase their business operations globally. As more organizations develop an international presence, these systems become a vital tool to promote and sustain organizational successes in the global marketplace. To be effective, IS professionals must understand globalization and how it relates to IS. Organizations such as the Association of Information Systems (AIS), Association of Computing Machinery (ACM), and Information Systems Audit and Control Association (ISACA) can provide information to stay abreast of the developments and opportunities (such as career, networking with IS professionals) related to the theory and practice of IS in the global environment. Establishing and maintaining global connections provides IS professionals with invaluable resources to accomplish IS goals.

Characteristics and Roles of Information Systems Professionals

People working in IS may be involved with new technologies applicable to information systems, how information systems are used globally, and the ethical requirements necessary to ensure a system is managed securely with integrity. IS professionals hold a variety of important roles and responsibilities in an organization. These include the following:

- A chief information officer (CIO) establishes and maintains an organization's overall information systems. The CIO's responsibilities include ensuring that the systems comply with legal requirements and that others involved in an organization's information systems do their jobs competently.
- Data information systems management manages the people, technology, and procedures needed to convert data into information. This includes cleaning, extracting, integrating, categorizing, labeling, and organizing data.
- Database management develops procedures to organize, manipulate, and retrieve data that are stored on computer databases.
- Systems analysis, design, and development examines an organization's system needs, and designs and develops a system to meet those needs.
- IS security risk management manages the risks that threaten an organization's information system.
- Enterprise security, data privacy, and risk management focuses on threats, such as data breaches, cyberattacks, and risks to data privacy, that can compromise an organization's data and information systems.
- Cloud computing focuses on how an organization uses information systems in the cloud for purposes such as storing and processing data.

- Data analytics and modeling transforms raw data into useful information and analyzes that data to provide information useful in organizational decision-making and other operations.
- IS project management uses the project management steps of initiation, planning, execution, monitoring, control, and closure to handle IS projects.

In addition to the benefit of working in a role aligned with an individual's experience and interest, IS positions tend to pay competitive salaries, and the field's outlook remains promising.

ETHICS IN IS

Ethics as Integral to IS

Any IS professional will likely have to manage sensitive data, and mishandling it can negatively impact the operations of organizations, as well as the lives of individuals. Cybersecurity is a priority because, worldwide, hackers are constantly working to find organizations with vulnerable systems that can be exploited for financial gain and other criminal uses. IS professionals must understand IS risks and practice ethical behavior to manage those risks. Keep in mind that every part of IS must be managed with an ethical mindset, understanding its importance and recognizing that IS professionals have an obligation to do everything they can to help safeguard data.

1.3 Connections between Information Systems and Information Technology

Learning Objectives

By the end of this section, you will be able to:

- Explain competencies in IS and IT
- Describe the connections between IS and IT
- Discuss training and education requirements for IS fields

As you have learned, organizations must have robust information systems managed by qualified professionals. To help ensure that IS professionals and organizations have the required expertise, the U.S. Department of Labor has developed the Information Technology Competency Model, a framework that defines the knowledge, skills, and abilities that are essential for IS professionals. It is important for IS professionals to understand the relationship between IS and IT, as these two disciplines work in tandem to support organizational objectives and foster innovation. Further, many of the training and education requirements for professionals in the IS field use the Information Technology Competency Model to prepare individuals to navigate the complexities of this dynamic and rapidly changing industry.

Competencies in IS

For all occupations, including IS positions, the U.S. Department of Labor (DOL) recommends competency-based approaches for hiring employees and for providing the education and training that employees need to do their jobs well. A **competency** is the ability to apply specific skills, experience, and personal characteristics to do a job in an effective and efficient manner. Someone's personal characteristics are the traits that are appropriate for the job or task being done based on the individual's interests, strengths, background, education, and training. In addition, an individual's talents, motivations, and personal perceptions of their work influence competency.

A **competency model** is a framework that identifies the competencies required for employees to effectively perform their job. Generally, for all industries, the competencies that are important include the following elements:

- Personal effectiveness: competencies such as interpersonal skills, integrity, professionalism, initiative,

dependability, reliability, and willingness to learn
- Academic: competencies such as reading, writing, and mathematics
- Workplace: competencies used in the workplace such as teamwork, creative thinking, problem-solving, and decision-making
- Industry-wide technical: general competencies needed in a specific industry; for example, database management and network administration are competencies necessary to succeed in IS
- Industry-sector technical: competencies directly related to specific positions within an industry; for example, in IS, professionals who focus on cybersecurity must be competent about data security and risk management
- Management: leadership, direction setting, team oversight, conflict resolution, delegation

To be successful in the workplace, IS professionals need personal effectiveness, academic, and workplace competencies. In addition, they need competencies specific to technology and information systems. These include knowledge and skills in the principles of information technology, databases and applications, technological networks, telecom, wireless and mobility, software development and management, user and customer support, digital media and visualization, compliance, risk management, security, and information assurance. IS professionals also need competencies specific to the role they fill in IS. Table 1.1 outlines both general and IS-specific professional competencies.

Competency	Description	Examples
Personal effectiveness	Personal characteristics or traits related to working	General: • interpersonal skills • initiative • dependability • reliability IS-specific: • integrity • willingness to learn • professionalism
Academic	Essential education	General: • reading • writing • mathematics IS-specific: • business • technology

Table 1.1 Professional Competencies No matter what field you go into, certain personal, academic, and workplace skills are needed to be successful as you grow in your career.

Competency	Description	Examples
Workplace	Competencies used in the workplace	General: • teamwork • creative thinking • decision-making IS-specific: • business fundamentals • problem-solving • listening
Technical	General competencies needed in a specific industry	IS-specific: • IS principles and concepts • IS standards and IS regulations • databases management • network administration • risk management
Occupation-specific	Competencies directly related to specific positions within an industry	IS specific: • cloud computing: networking, programming, machine learning, virtualization, cloud security, business concepts, and project management • systems analysis: system design, data analysis, business analysis, problem-solving, critical thinking, creativity, and systems administration • cybersecurity: threat detection systems, digital forensics, penetration testing, auditing, data security, data privacy
Management	Competencies regarding leadership, conflict resolution, delegation, and team dynamics	General: • team management • conflict management • delegation • leadership IS-specific: • risk assessment • policy development • regulatory compliance • incident response planning

Table 1.1 Professional Competencies No matter what field you go into, certain personal, academic, and workplace skills are needed to be successful as you grow in your career.

LINK TO LEARNING

As a student, you can use the Department of Labor's (DOL's) Information Technology Competency Model (https://openstax.org/r/109DoLInfo) to understand the knowledge you should gain and the skills you should develop to have a successful career in IS.

Connections between Information Systems and Information Technology

As an IS professional, you likely will work closely with professionals in IT. Although the terms *IS* and *IT* are sometimes used interchangeably and the fields are connected, they are not the same. While IS focuses on an organization's goals and developing an information system to meet organizational needs, IT is concerned with the technological operations. IT professionals design and build an organization's technological infrastructure, including the computer hardware, software, and networks required to support the information system. IT professionals also provide user support to maintain technology and ensure that it functions appropriately.

IS and IT professionals typically work together to ensure that an organization's technological needs are met. For example, IT professionals use IS requirements to guide their work as they design and develop an organization's technological infrastructure.

LINK TO LEARNING

You will likely work with IT professionals at some point during your career, and it will be helpful to understand how IT roles differ from IS roles. This geeksforgeeks.org blog provides more details (https://openstax.org/r/109ITvsIS) about the differences, including a table that compares the two fields.

Career Focus: Training and Education Requirements for Information Systems Fields

If you are interested in becoming an IS professional, or just want a better understanding of the impact of IS on organizations, you will benefit from learning about a variety of topics important in business and technology. Some of the key topics include the following:

- **business analysis**, which reviews an organization's operations to determine needs and how these can be addressed by IS
- cybersecurity, which identifies an organization's cybersecurity risks and implements measures for risk management
- **enterprise system**, which is a software package that organizations use to automate and coordinate operations, solve an organization's problems, and monitor organizational performance
- information system design, which develops the framework and structure for IS that enables IS to meet an organization's specific needs
- **information technology (IT)**, which reviews how computers and other technology can be used to process, store, retrieve, and share information
- networks, which explores the processes to connect computers and other technology to enable information sharing
- programming, which delves into the processes to develop and write computer code that enables hardware and software to function appropriately

If you want to pursue a degree in IS or learn more about specific topics, you can take additional courses devoted to covering these subjects in depth.

Depending on the role, future IS professionals may qualify for a job by earning a degree or certification(s) in IS, or both. Even if an IS professional has a degree, earning certifications can provide additional knowledge and training in areas such as security, database management, and data analytics. With certifications, IS professionals are required to complete continuing education credits each year, and holding one or more certifications signals that an IS professional is dedicated to their work. The certifications held by IS professionals include Associate Computing Professional (ACP), Business Data Management Professional (BDMP), Certified Business Intelligence Professional (CBIP), Certified Data Professional (CDP), and Information Systems Analyst (ISA). Typically, IS professionals earn the certification(s) related to the IS role(s) that they perform. To learn more, refer to 5.4 Career Focus: Key Certifications.

1.4 The Global Importance of Information Systems

Learning Objectives

By the end of this section, you will be able to:

- Describe why information systems should be global
- Discuss global innovation and its importance
- Describe global initiatives in IS

The field of IS is and has been an important component in **globalization**, or the process of businesses and other organizations operating around the world. This includes the international sales of goods and services, as well as the exchange of ideas across international borders.

Why Information Systems Should Be Global

The global marketplace is an important resource worldwide. Countries trade goods and services, offering businesses around the world opportunities for growth and profit maximization. Organizations of all types in both the private and public sectors use globalization as a means to share information and resources, including technological knowledge.

IS supports globalization by providing the resources that organizations need to achieve success in the global marketplace. This includes enabling global communication and information sharing, as well as supporting the processes to manage data compiled from sources throughout the world. IS also gives organizations the tools to function at any time of day, eliminating the need for different time zones to be an obstacle in global operations. In addition, IS helps organizations develop the frameworks they need for strategic planning and decision-making on a global scale.

You will learn more about globalization and the role of IS in promoting global operations in Chapter 11 Global Information Systems which covers strategic and global information systems. This will include a look at the role of culture in IS, as well as IT, and the risks associated with the use of global data and systems sharing. For now, it is important to recognize IS as a vital tool for globalization.

Global Innovations

One role of IS is to support and promote **global innovation**, which refers to the processes used to collaborate across international borders in designing and developing new goods and services for the global marketplace. Global innovation also focuses on international collaboration to develop solutions for global problems and challenges, such as climate change. For example, the World Meteorological Organization (WMO) helps governments and other organizations throughout the world track climate change and gather the information needed to make decisions, set policies, and take action to combat the impacts of climate change.

Organizations use processes such as business analysis, problem-solving, and decision-making for global innovation, and these same processes are used for internal and local issues. With global innovation, these organizational processes have a broader scope as they are applied to the global marketplace and this is covered in-depth in Chapter 11 Global Information Systems. In addition, Chapter 10 Emerging Technologies and Frontiers of Information Systems explores topics relevant to global innovation including emerging technology, the evolving frontiers of IS, and the future of technology and its impacts on IS.

FUTURE TECHNOLOGY

Artificial Intelligence: Theory in Action

Technology changes rapidly, and IS professionals must stay abreast of technological advances, understanding the impact that these have on IS. For example, consider artificial intelligence. AI has many potential benefits for IS, including improvements in efficiency for the processes to gather, store, and manage data. AI also presents a number of serious challenges such as privacy concerns as AI often gathers data without the individual's consent. AI is rapidly evolving and will be an important part of the future of IS. The advent of AI also provides an example of why continuing education is so important. With continuing education, IS professionals can ensure that they are prepared to handle the future, regardless of what technological changes and challenges face them.

Global Initiatives in Information Systems

As technology advances throughout the world, IS must continue to evolve. The key topics IS professionals are following include artificial intelligence, machine learning, 5G and the Internet of Things, edge computing, and blockchain.

- The ability of machines and computers to act, reason, and learn, continuing to develop and evolve, is called artificial intelligence. AI has various applications for IS. For example, AI can help process and manage data, making IS more efficient. This includes automating processes and reducing errors, ensuring that organizations have more accurate and reliable data for decision-making and other purposes. AI also can help organizations detect security threats and identify security issues more quickly, making it easier to protect an organization's information.
- The type of AI that allows machines to imitate human thought by improving and learning from experiences without explicit instructions or programming is called machine learning. ML also is evolving and changing the way IS is managed. For example, ML promotes more efficient and accurate processing of the data analytics and documentation needed in IS. As with AI, ML also can help with cybersecurity.
- During the advancement of 5G, the fifth generation of cellular network technology, and the Internet of Things (IoT), the network that connects everyday physical objects to the internet, enabling them to collect and share data with other devices or systems, IS is experiencing changes, such as the faster exchange of information and greater network connectivity. IoT also helps with real-time data collection and automation, which can improve the information available for IS.
- The distributed computing framework that allows data storage closer to the source of data, rather than a centralized cloud or server, is called edge computing. It is continually advancing, giving IS greater options for storing and processing data.
- The shared ledger that records transactions and is maintained through linked computers in a peer-to-peer network is called blockchain. Originally developed in 2008 for Bitcoin, it allows information systems more ways to store and share data with increased efficiency and security.

As technology advances, IS faces more risks, and this creates additional challenges to cybersecurity. Cybercriminals and cyberattacks are on the rise. According to the Federal Bureau of Investigation, 2023 saw a record number of complaints about cybercrimes, with over 880,000 complaints and financial losses exceeding $12.5 billion. This was a 10 percent increase in complaints and a 22 percent increase in financial losses compared to the previous year.[4] Fighting cybercrime and developing better cybersecurity to handle technological advances is an important global initiative for IS professionals throughout the world.

4 Internet Crime Complaint Center, *Internet Crime Report* (Federal Bureau of Investigation, 2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

LINK TO LEARNING

One way to learn more about IS in cybersecurity and understand its importance is to play security awareness games. You can give this a try by exploring the Security Awareness Games (https://openstax.org/r/109SecurtyGames) from the Center for Development of Security Excellence. The website also offers games, word searches, and crossword puzzles that can help you learn more about cybersecurity.

Key Terms

Agile methodology framework used to guide project management, primarily by dividing projects into phases, or sprints

American Society for Industrial Security (ASIS) global organization that provides training and certification to help professionals in IS and other technological industries provide security for people, property, and information

application control control that is built into a system and includes features such as firewalls, encryption, and access control

application software program that enables computers to perform specific tasks

business analysis understanding what a business needs to avoid or solve a problem or to take advantage of an opportunity

competency ability to apply specific skills, experience, and personal skills to do a job in an effective and efficient manner

competency model framework that identifies the competencies required for employees to effectively perform their job

control policy or procedure that ensures an information system functions effectively, efficiently, and securely

Control Objectives for Information and Related Technologies (COBIT) framework that develops and maintains an information system using five processes: Evaluate, Direct, and Monitor (EDM); Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA)

data raw facts and figures that are processed and turned into meaningful information

data capture process of gathering data from various sources, such as customers and financial records, and inputting this data into an information system

data dissemination process of distributing and sharing information, such as reports, videos, photographs, and other information system outputs

data processing using calculations, manipulations, and analysis to transform data into useful information

data storage process of maintaining the data and information of a system in a location that is secure, reliable, and accessible to authorized users

decision support system (DSS) system that assists in decision-making by providing interactive tools and access to data analysis

digital media content developed, stored, and distributed via mobile devices—such as news stories, blogs, videos, and online games—as well as the hardware—flash drives, DVDs, and digital computers—used to store and share this media

enterprise resource planning (ERP) system type of information system used by everyone in an organization to integrate various business processes and functions across an organization such as human resource management and inventory control

enterprise system software package an organization uses to automate and coordinate operations, solve the organization's problems, and monitor organizational performance

environment factors such as physical location and network capabilities that affect an information system and help determine how it operates

executive information system (EIS) (also, strategic information system, or SIS) system that supports the strategic information needs of top executives

Federal Information Security Modernization Act (FISMA) sets guidelines and standards for security that organizations are required to meet to minimize the possibility that data will be stolen, lost, or misused

feedback information that users provide to managers about an information system's functionality

field of information systems (IS) dynamic industry, evolving and depending on technological advancements, that intersects with business, computer science, and management, playing a critical role in enhancing organizational efficiency, productivity, and competitiveness

framework structured set of guidelines and best practices that is used to guide the process of developing, implementing, managing, or maintaining a business process, policy, system, or procedure

general control process that outlines how an information system is to be used and includes requirements such as routine password updates

global innovation processes used to collaborate across international borders in designing and developing new goods and services for the global marketplace

globalization process of businesses and other organizations interacting on a global scale

hardware physical devices such as computers, servers, networks, and storage devices that are used to collect, process, and store data

industry standard policy, procedure, or requirement widely used and supported in an industry to promote efficiency and quality in goods and services

information raw data that have been processed and manipulated to give context and meaning

information system set of interconnected components that integrate the collection, processing, storage, and distribution of data, information, and digital products

information technology field that reviews how computers and other technology can be used to process, store, retrieve, and share information

Information Technology Infrastructure Library (ITIL) comprehensive framework of documentation that discusses best practices for managing information technology

input data that are collected and entered into the system by users or automatically when transactions occur

IS2020 competency model that provides guidance and standards that undergraduate IS programs should meet to ensure students are prepared for careers in IS

ISO/IEC 27001 worldwide standard established by the International Organization for Standardization that defines the requirements information systems must satisfy to provide adequate security for any system

management information system (MIS) system that provides middle managers with reports and summaries to support decision-making

McKinsey 7-S Framework focuses on how an organization can be efficient and effective with interaction and coordination of its staff, structure, strategy, skills, systems, style, and shared values

operating system (OS) functions as a computer’s manager by operating a computer’s memory and other hardware resources such as disk storage; provides the interface that users need to work with a computer and manages a computer’s application software programs

output data or information that a system generates and provides to users

procedure set of instructions and rules that governs the use of the hardware, software, and data components in information systems

processing performance of tasks in order to make data useful in a system

qualitative data nonnumerical information

quantitative data numerical information

Skills Framework for the Information Age (SFIA) provides a comprehensive skills and competency framework in a common language for the IT industry

social media any type of electronic communication tool that enables users to establish online communities where they share content, including personal messages, ideas, photographs, and videos

software programs and applications that run on computer hardware, enabling users to perform specific tasks

The Open Group Architecture Framework (TOGAF) standard that promotes best practices for information systems and other technology

transaction processing system (TPS) system that handles day-to-day transactions such as order processing and payroll

Waterfall structured, linear framework used to guide project management

Zachman Framework provides a structure for developing and organizing the artifacts of enterprise architecture, including data and documents

Summary

1.1 Introduction to Information Systems

- An information system refers to a set of interconnected components that integrate the collection, processing, storage, and distribution of data, information, and digital products in order to support decision-making, coordination, control, analysis, and visualization in an organization.
- Information systems can be categorized into different types based on their scope and functionality, including executive information systems used by an organization's executive staff, decision support systems used by senior managers, management information systems used by middle managers, and transaction processing systems used by frontline workers. In addition, everyone in an organization typically uses enterprise resource planning (ERP) systems for functions such as project management, accounting and financial management including payroll, and tracking customer service.
- An information system typically consists of five key components—people, data, procedures, hardware, and software.
- The basic purpose of information systems—processing and sharing information—has been part of our communication practices since the beginning of civilization, evolving from simple cave drawings to the complex technology we have today.
- The printing press, telegraph, and telephone laid the technological foundation for the communication tools used in today's complex information systems.
- While societies developed a variety of methods for communication, they also created tools for calculations, establishing the foundation for modern computers. The abacus from at least 1100 BCE, analog and digital calculators invented in the 1600s, and the Jacquard loom invented in the early 1800s, provided the foundation for the computers used in today's complex information systems.
- Once the components of information systems are in place, the elements of environment, input, processing, output, control, and feedback are necessary for the information system to function.
- Information system operations refer to how the system is used and includes data capture, processing, storage, retrieval, and dissemination.
- Organizations have come to rely on the field of information systems as a critical resource. A well-developed and maintained information system offers many benefits, including improved efficiency, more robust decision-making, enhanced communication processes, increased productivity, and competitive advantages.

1.2 Frameworks of Knowledge and Industry Standards

- To promote best practices and help organizations achieve information systems goals and objectives, the field of IS is guided by frameworks and industry standards.
- Frameworks help IS professionals apply critical thinking, promote proactive communication, guide IS professionals as they organize their ideas, provide a foundation for strategic planning, and provide IS professionals with resources such as continuing education, best practices, and guidelines for information systems operations.
- Industry standards help IS professionals ensure that the system they develop has the appropriate infrastructure and technological components required to function efficiently.
- Common frameworks applicable to IS include Agile, COBIT, ITIL, McKinsey 7-S, SFIA, Waterfall, and Zachman.
- Industry standards that are applicable to IS include ASIS, FISMA, IS2020, ISO/IEC 27001, and TOGAF.
- IS professionals perform many roles in organizations, including data information systems management; database management; systems analysis, design, and development; security risk management; enterprise security, data privacy, and risk management; cloud computing; data analytics and modeling; and project management.

1.3 Connections between Information Systems and Information Technology

- To help organizations meet IS needs, the U.S. Department of Labor has developed the Information Technology Competency Model, a framework that defines the knowledge, skills, and abilities that are essential for IS and IT professionals.
- Key competencies include personal effectiveness, academics, and workplace behaviors such as teamwork and decision-making.
- DOL also identified technical competencies, which refer to skills and abilities needed in a specific industry. For IS professionals, these include the principles of information technology, databases and applications, technological networks, telecom, wireless and mobility, software development and management, user and customer support, digital media and visualization, compliance, risk management, security, and information assurance.
- While IS and IT are connected and the terms are sometimes used interchangeably, they are not the same. IS focuses on an organization's goals and developing an information system to meet organizational needs. IT is concerned with technological operations and designing and building an organization's technological infrastructure, including the computer hardware, software, and networks required to support the information system.
- To become an IS professional, students should learn about various topics important in business and technology, including business analysis, cybersecurity, enterprise systems, information system design, information technology, networking, and programming.
- In addition to a degree, IS professionals may want to pursue certification. The certifications held by IS professionals include Associate Computing Professional (ACP), Business Data Management Professional (BDMP), Certified Business Intelligence Professional (CBIP), Certified Data Professional (CDP), and Information Systems Analyst (ISA).

1.4 The Global Importance of Information Systems

- IS has and continues to be an important component in globalization as IS provides the resources organizations need to achieve success and innovation in the global marketplace.
- As technology advances throughout the world, IS must continue to evolve. The technologies that impact IS include artificial intelligence, machine learning, 5G, the Internet of Things, edge computing, and blockchain.
- As technology advances, IS also faces more risks that create additional challenges to cybersecurity.

Review Questions

1. What type of information system is used by everyone in an organization to integrate various business processes and functions across an organization?
   a. management information system (MIS)
   b. enterprise resource planning (ERP)
   c. transaction processing system (TPS)
   d. decision support system (DSS)

2. What invention is credited with providing ordinary people with access to information and ideas that were previously unavailable?
   a. telegraph
   b. telephone
   c. printing press
   d. internet

3. What invention provided a vital framework for the development of computers?
   a. Jacquard loom

   b. printing press
   c. digital calculators
   d. typewriters

4. What do computers require to manage the computer’s memory and other resources such as disk storage while providing the interface for computer users?
   a. application software
   b. operating system software
   c. hardware
   d. data processing

5. What element of an information system is concerned with the policies and procedures that ensure an information system functions effectively, efficiently, and securely?
   a. processing
   b. environment
   c. feedback
   d. control

6. You are the project manager of a team of IS professionals working together to develop an information system, and you need a suitable structure to guide your team’s work. What is this structure called?
   a. guideline
   b. best practice
   c. framework
   d. industry standard

7. As your team works to develop an information system, they review the policies, procedures, and requirements that apply to your organization’s system. What are they reviewing?
   a. guidelines
   b. best practices
   c. frameworks
   d. industry standards

8. As the member of a team developing the information system for your organization, you have been assigned to review best practices and make recommendations to the team on which best practices are most applicable to your organization’s system. What resource do you use to access the most comprehensive information on best practices?
   a. Agile
   b. ITIL
   c. SFIA
   d. COBIT

9. When IS professionals work for a government agency or a private business that contracts with the government, what must they follow to meet system security requirements?
   a. COBIT
   b. ITIL
   c. FISMA
   d. ISO/IEC 27001

10. Your new job in IS requires you to transform raw data into useful information that your organization can use in decision-making and other operations. What is your job?
   a. data analytics and modeling
   b. cloud computing
   c. database management

d. IS project management

11. Imagine you are part of the hiring team tasked with filling your organization's IS jobs. You are concerned about one of the candidates recommended by a coworker because you do not agree that this person has the integrity, initiative, and willingness to learn required for the role. What competency do you think this candidate is lacking?
    a. academic
    b. workplace
    c. technical
    d. personal effectiveness

12. Your colleague has excellent skills in teamwork, creative thinking, and problem solving. What competency does your colleague have?
    a. academic
    b. workplace
    c. technical
    d. personal effectiveness

13. What is the main focus for an IT professional?
    a. organizational goals
    b. technological infrastructure
    c. organizational competencies
    d. business analysis

14. What key topic in IS education refers to the software packages that organizations use to automate and coordinate operations, solve an organization's problems, and monitor organizational performance?
    a. enterprise systems
    b. information system design
    c. programming
    d. business analysis

15. What key topic in IS education explores the processes to connect computers and other technology to enable information sharing?
    a. enterprise systems
    b. information system design
    c. networks
    d. information technology

16. What is the process of collaborating across international borders to design and develop new goods and services for the global marketplace?
    a. globalization
    b. global initiative
    c. global innovation
    d. global computing

17. What is artificial intelligence (AI)?
    a. the ability of machines to imitate human behavior
    b. a type of advanced calculator
    c. a new programming language
    d. a method for speeding up computer processors

18. What is an example of a good application for blockchain?
    a. recording data that is subject to change
    b. health-care records

c. information sharing between companies
d. money transfer

Check Your Understanding Questions

1. In an information system, what is the difference between hardware and software?
2. How did the telegraph and telephone lay the groundwork for the invention of the internet?
3. Explain the differences between data capture, data processing, and data dissemination.
4. What was the intent behind creating the ARPANET and why was it important?
5. How can frameworks help IS professionals do their work efficiently and effectively?
6. As a student pursuing an undergraduate degree in IS, you want to know whether your school relies on industry standard IS2020 for guidance. Why is this important?
7. You are tasked with maintaining the infrastructure to provide security for your organization's information system. As part of this process, why would you rely on standard ISO/IEC 27001 for guidance?
8. The manager of your organization argues that using DOL's competency models to guide the hiring process is too much work. What do you say to convince your manager that using the competency models can benefit your organization?
9. Why do technological advances pose risks for IS?

Application Questions

1. A friend asks you to explain the concept of information systems and why it is important for organizations. What do you say?
2. Your business offers more than fifty products for sale. Currently, you have a bookkeeper who uses a laptop with a basic spreadsheet program to track orders and maintain business records. You have five other employees who handle tasks such as inventory management and sales, but your business is small, and the only person who has computer access is the bookkeeper. Explain at least three ways an information system could benefit your business.
3. One of your colleagues does not understand why industry standards are important in IS. What do you say to help this colleague understand industry standards and how they can benefit IS?
4. What is SFIA and how can it help your organization establish and maintain a robust information system?
5. You are explaining your new job in IS to a friend who does not understand how your job differs from an IT job. Explain the difference between IS and IT to your friend.
6. The manager of your organization argues that there is no need for your organization's information system to be concerned about globalization. What do you tell your manager to explain why the information system should be global?

2

Data Management and Information Systems Business Strategies

Figure 2.1 As technology advances, businesses and other organizations have many tools available to promote efficient operations. Robust data and information management strategies are necessary to ensure that these technological tools function optimally. (credit: modification of work "Voigtländer Vitoret - AZ Tower 3" by Jaroslav A. Polák/Flickr, CC0 1.0)

Chapter Outline

Introduction

The days when organizations relied on paper files and simple data processing programs to maintain records and conduct business are long past. Technological advancements have given organizations the capability to handle massive amounts of data in a digital environment. Data provide organizations with vital information to improve efficiency and support competition in the marketplace. Businesses and other organizations must manage data and information effectively to promote their success and to avoid data inaccuracies, noncompliance with legal requirements, lost opportunities, increased costs, and dissatisfied customers. How organizations develop and maintain robust data and which systems they utilize are important to organizational success.

2.1 Practices and Frameworks for Data Management

Learning Objectives

By the end of this section, you will be able to:

- Identify practices and frameworks in the management of data
- Interpret the dimensions and characteristics of data needed to make decisions
- Identify information system planning strategies and frameworks that inform an organization's data management practices and processes

Organizations typically use digital technology to analyze data to get the information they need to run their businesses. With the exponential increase in computing capacity and the development of artificial intelligence (AI) and large-language models, businesses today rely heavily on efficient managers using sophisticated data storage and data analytics technologies. How can you align your organization’s data management and information strategies to deliver optimal results for the greatest number of stakeholders? Future data managers will have an obligation not only to understand information and data management but also to possess the ability to extract valuable insights from data, apply these insights strategically, and align them with the organization’s goals.

In Chapter 1 Fundamentals of Information Systems, you learned that the term data refers to raw facts and figures that are processed and turned into meaningful information. Data represent discrete elements without context or meaning on their own, and data come in various forms—such as numbers, text, images, or audio. For example, a list of numbers or a collection of customer names and addresses is considered data. Information is the result of processing data through organization, analysis, and contextualization to derive meaning. If the data are a list of numbers, then the related information may be the trend of increasing sales of a product. This information can be used to make decisions, understand relationships, and gain insights.

For any organization, information is an invaluable resource, hence data and data management have become critical. Effective data management aligns with data analytics capabilities, facilitating the automated discovery of trends, patterns, and anomalies through techniques like data mining and analysis. In today’s data-driven world, there’s increasing attention to the relevance of **big data**, highly complex and large datasets that require specialized processing techniques to extract valuable insights and make informed decisions. Managing any data involves activities such as cleaning, extracting, integrating, categorizing, labeling, and organizing. All these activities should be executed in a manner that ensures that the quality of the data is preserved, and the data remain secure but also easily retrievable. Organizations need people to manage data and control data accessibility, and they need to define roles and responsibilities for all the people working with and extracting information from their data. Decisions about data management have long-lasting impacts, so it is important for organizations to select suitable frameworks for managing data.

Identifying Practices and Frameworks That Assist Data Management

Analysts report that by 2025 the global volume of data is expected to reach 200 zettabytes.[1] A zettabyte is a measure of digital storage capacity equal to a thousand exabytes, a billion terabytes, or a trillion gigabytes. Notably, most of these data are underutilized. For most enterprises, only about one-third of data is used for decision-making, while the remaining two-thirds is simply stored.[2] When analysts are unable to find the appropriate and available data for decision-making, it can cost organizations billions of dollars each year. On the other hand, data archives are often required for regulatory reasons to ensure compliance with laws governing data retention, privacy, and security. For instance, industries like health care and finance have strict regulations regarding the retention of patient records and financial transactions data.

Another important aspect of dealing with data is **data governance**, which involves the policies, procedures, and standards how an organization manages the availability, usability, integrity, and security of its data throughout the data life cycle. You probably have noticed that every time you use the internet, an app on your phone, or buy something online, websites and apps track what you do, and may track your location and other data. The world is full of sensors, electronic payments, tracking data, biometric information like fingerprints, and smart home devices that collect data. This kind of information is valuable, and this creates challenges for making sure data are handled well. Data governance is like a rulebook for how data are managed and making sure the right people are responsible for decisions about data.

1 Steve Morgan, “The World Will Store 200 Zettabytes of Data by 2025,” *Cybersecurity Magazine*, February 1, 2024, https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
2 “Wasted Data: Why So Much Enterprise Information Goes Unused,” MarketLogic, October 26, 2022, https://marketlogicsoftware.com/blog/wasted-info-why-so-much-enterprise-data-goes-unused/#:~:text=Unbelievably%2C%20only%20about%20one%20third,their%20data%20remains%20%E2%80%9Cdark%E2%80%9D

Appropriate data management is crucial to an organization's reputation and success. Data management parameters establish practices that organizations can use to ensure that their data are managed, protected¸ and of high quality so they can be utilized to make informed decisions. The essential areas for managing data effectively are as follows (Figure 2.2)[3] :

- Data governance establishes policies, processes, standards, roles, and responsibilities to manage data as a valuable asset.
- Data quality ensures that data are accurate, complete, and consistent. This is achieved through activities such as validation, cleansing, matching, and monitoring via metrics and reporting.
- Data integration combines data from different systems and applications. It includes tasks such as mapping data elements, transforming data, and ensuring seamless integration using tools and best practices.
- Data security protects data from unauthorized access, use, disclosure, disruption, modification, or destruction. It is achieved through measures like encryption, access controls, and adherence to security best practices.
- Data privacy, like data security, safeguards personal data from unauthorized access, use, disclosure, disruption, modification, or destruction. It relies on the use of encryption, access controls, and privacy best practices.
- Data retention involves storing data for a defined period based on legal, regulatory, and business requirements. It includes activities like archiving, purging, and the development of data retention policies.
- Data architecture focuses on designing data models and database structures that align with business needs.
- Data analytics involves analyzing data to extract insights and support decision-making. It includes implementing activities like data warehousing, mining, and visualization to achieve meaningful information extraction. These tools, techniques, and insights can be used in AI and machine learning applications. (George Firican, ”Data Management Framework 101”)

3 George Firican, "Data Management Framework 101," *LightsOnData*, https://www.lightsondata.com/data-management-framework/

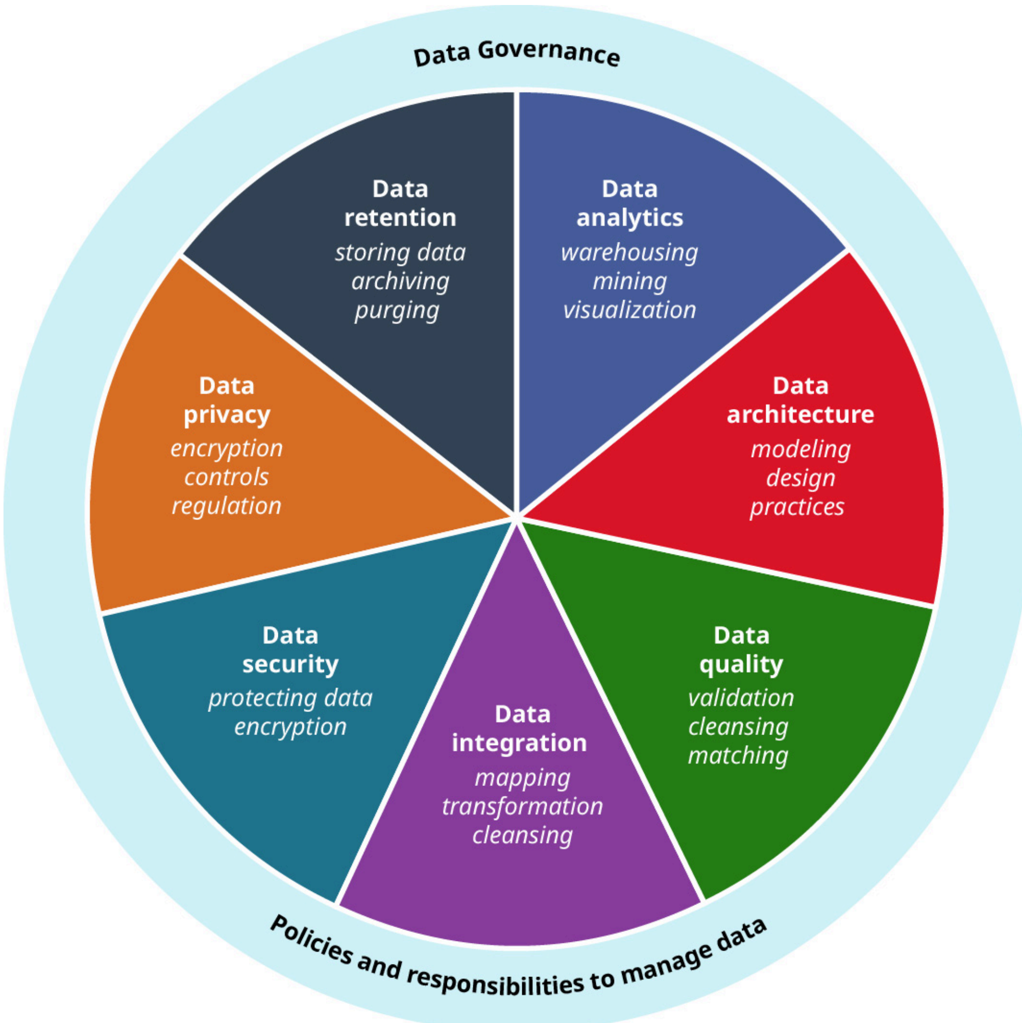


Figure 2.2 Data governance plays a role in all data management areas. It ensures an organization's data are of high quality and are managed and protected effectively so that the data can be used to make informed decisions. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

FUTURE TECHNOLOGY

Data Management Technologies

A new approach to data management, called a data mesh, is based on the principle of domain-driven design. In a data mesh, data are owned by the domain experts who create the data, and the data are made available to other users through a self-service model.

Another powerful technique for data management is called data fabric. It involves a move toward data democratization, which means that data are made available to more people in the organization, not just those in information technology (IT) or data science roles. Through this approach, data can be accessed and consumed by anyone as long as they have proper security credentials for the level of data they desire.

Another technology is federated analytics. Federated analytics allows users to analyze data without having to move it to a central repository. This can help to improve data security and privacy, and it can also make it easier to analyze data that reside in different locations. These three techniques address the growing complexity and scale of data management in modern organizations, especially as data becomes more distributed, diverse, and decentralized. These technologies provide innovative ways to manage, integrate, and analyze data at scale, which is necessary in the age of big data and advanced analytics.

Businesses that strive to ensure they follow these data management parameters can decide to follow any framework. A framework is a structured and organized approach that provides a set of guidelines, principles, or tools to address complex problems or tasks in a systematic manner. It serves as a foundation to build and manage processes, systems, or projects, ensuring consistency, efficiency, and effectiveness. Following are some common data management frameworks:

- DAMA-DMBOK: The Data Management Body of Knowledge, developed by the Data Management Association (DAMA International), provides comprehensive guidelines across ten key knowledge areas, including data governance, data architecture, and data quality.
- MIKE2.0 IMM: This framework offers a structured way to assess an organization's information maturity level.
- IBM Data Governance Council Maturity Model: This model provides a road map for implementing effective data governance processes and controls.
- Enterprise Data Management (EDM) Council Data Management Maturity Model: This comprehensive framework covers various aspects of data management, including data strategy, data operations, and data architecture.
- Responsible Data Maturity Model: This model is an evolving concept that continues to gain importance as the role of data in our lives becomes more prominent.

There are some differences in how each framework approaches data management. DAMA-DMBOK focuses on the technical aspects of data management, while MIKE2.0 focuses on the business aspects of information management. The IBM Data Governance Council Maturity Model and the EDM Council Data Management Maturity Model are both designed to help organizations assess their current data management practices and identify areas for improvement. The best framework for an organization will depend on its specific needs and requirements. However, all five frameworks can be valuable tools for improving data management and information quality. The optimal framework for managing data is one that is continuously developing to address advancements in data storage and changes in organizational policy.

CAREERS IN IS

Data Architect

A data architect is responsible for designing, creating, and managing an organization's data architecture. This includes creating frameworks and structures for collecting, storing, processing, and accessing data in a way that aligns with business goals, compliance requirements, and performance needs. In addition to designing traditional data architectures, many modern data architects now also focus on frameworks like data mesh, data fabric, and federated analytics as part of their responsibilities. A data architect needs strong knowledge of database technologies, data modeling, cloud platforms, and big data tools. They must also understand data governance practices, security protocols, and compliance regulations and be familiar with data pipelines, integration tools, and extract, transform, and tools. Having strong problem-solving skills will allow a data architect to design complex systems and solve integration challenges, ensuring data flows smoothly across different parts of the organization.

Most data architects have a bachelor's degree in computer science, information systems, business analytics, or a related field. Some also have a master's degree, which can help give candidates a competitive edge or allow for a smoother transition from another field. There are also numerous certificates available for a data architect. Different organizations may require different certifications, but the Certified Data Management Professional certificate is one that many organizations prefer.

To become a data architect, you typically need a combination of a strong educational foundation, hands-on experience working with data systems, and certifications in specialized tools and platforms. Ongoing learning and keeping up with industry trends are also helpful in this rapidly evolving field.

Dimensions and Characteristics of Data to Inform Data Management Decisions

For each type of data, an organization needs to define rules and policies to measure the quality of the data and the effectiveness of the data's management. There are four key dimensions of big data known as the four *V*s:

- Volume: The dimension of **volume** refers to the vast amount of data generated and stored. Big data datasets are incredibly large and can grow exponentially.
- Variety: The **variety** dimension encompasses the diverse array of data types and formats, which might include structured elements like user IDs, time stamps, and actions taken, as well as unstructured components such as user comments and feedback.
- Velocity: The rapid pace at which data are generated and collected, thereby necessitating real-time processing, is characterized by **velocity**. Particularly evident during high-traffic events, such as online flash sales, the constant influx of clickstream data necessitates swift analysis to enable the system to offer tailored recommendations and insights to users navigating a dynamic digital landscape.
- Veracity: The **veracity** dimension refers to the reliability, accuracy, and trustworthiness of the data, considering factors like data quality and consistency. As data originate from a multitude of sources and are influenced by user behaviors and tracking nuances, ensuring the quality of the data is imperative to avoiding misinterpretations of metrics like bounce rates and session durations.

Different types of data are required for generating suitable information, and different types of data require different management approaches. There are two main categories of data—structured and unstructured. The first, structured data, exist in organized, fixed fields in a data repository. Structured data are typically defined in terms of field name and type (such as numeric or alphabetical). Structured data can be further categorized as follows:

- Associated with operational or real-time applications, **operational data** include transactional data generated by day-to-day business operations. Operational data often require high availability, real-time processing, and quick access for operational decision-making. When managing operational data, the focus is on ensuring data integrity, availability, and performance to support critical business processes.
- Serving as a system of record or reference for enterprise-wide use, **master data** represent core entities such as customers, products, or employees, and **reference data** include codes, classifications, or standards used across the organization. Maintaining data accuracy, consistency, and synchronization across multiple systems for these data types is necessary to ensure reliable and consistent information across the organization.
- Used for data warehousing, business intelligence, and analysis-oriented applications, **analytic data** include aggregated and summarized data from various sources and enable in-depth analysis, reporting, and decision support. Analytic data require data integration, transformation, and optimization to provide a consolidated view and support complex analytics.

The other data type, unstructured data, do not reside in a traditional relational database; examples of unstructured data generated within organizations are emails, documents, media (videos, images, audio), slide presentations, social media activity (such as posts, images, ratings, and recommendations), and web pages. There are several challenges associated with managing unstructured data. Their large volume can make them difficult to store and manage. Unstructured data also come in a variety of formats from multiple sources, including internal sources, personal sources, and external sources. Data can also come from the web in the form of blogs, podcasts, tweets, social media posts, online videos, texts, and radio-frequency identification tags and other wireless sensors. These technologies generate data that must be managed but are difficult to process and analyze. Unstructured data are often generated at high velocity. This can make it difficult to keep up with and make sense of the data.

Despite the challenges, managing unstructured data can be valuable. Unstructured data can provide insights into customer behavior, identify trends, and improve decision-making. The management of unstructured data involves organizing, storing, and retrieving such content effectively. Techniques like content indexing, search, and metadata management are employed to enable efficient discovery and retrieval of relevant information. When managing unstructured data, it is also important to understand the decision-making priorities of an organization (which decisions require data and, consequently, necessitate data-driven information and knowledge processing). Also, it is often possible to convert unstructured data into structured data.

Good data management strategies require the following:

- Updating outdated data: A data management process should involve incorporating the latest information and revisions into the dataset, thereby ensuring it remains relevant and accurate.
- Rectifying known inaccuracies: Identifying and correcting any inaccuracies or errors in the data are crucial to maintaining **data integrity**, which means ensuring data remain accurate, consistent, and reliable over their entire life cycle.
- Addressing varied definitions: Dealing with diverse definitions across different data sources requires establishing a clear and standardized **data definition**, which is the instruction for how to organize information. These definitions tell a computer system what kind of data to expect (text, numbers, dates) and how the data should be formatted mapped to ensure consistency. For example, when the underlying data point is the same (the person's date of birth), the specific term used ("Date of Birth" versus "Birth Date") might differ based on the department using the data. However, the definition of the data point (the actual date) needs to be consistent throughout the system to ensure accurate analysis and reporting.
- Resolving discrepancies in redundant data sources: When multiple sources provide similar data, it is important to reconcile any inconsistencies or differences to establish a reliable and accurate representation of the information.
- Managing variations in opinions, forecasting techniques, or simulation models: Recognizing and addressing divergent viewpoints, methodologies, or models used for forecasting or simulation ensures transparency and reliability in the data analysis process.

FUTURE TECHNOLOGY

Master Data Management

Master data management (MDM) ensures the creation and maintenance of a single, accurate source of truth for crucial data points within an organization. This centralized data repository eliminates inconsistencies and fosters seamless information exchange across different systems and applications. Let's explore the importance of MDM in two specific contexts: health care and e-commerce retail.

- In the health-care sector, creating a unified, digital infrastructure for health-care services facilitates the seamless exchange of health-related information among patients, health-care providers, and government agencies. Efficient MDM ensures that patient data, such as medical history, medications, and allergies, are organized, stored securely, and readily accessible by authorized personnel. This both improves the efficiency of health-care delivery and reduces the risk of errors and delays in treatment.
- In the e-commerce sector, consider a large online retailer managing millions of product listings. Without MDM, product information like descriptions, specifications, and prices might be scattered across different data sources, potentially leading to inconsistencies. Master data management establishes a centralized repository for product data to ensure that customers see accurate and consistent information across all interfaces: web, mobile, on-site, and in marketing materials. Additionally, MDM facilitates efficient inventory management and product updates across various sales channels.

Information System Planning and Management

Information systems play an important role in data management by transforming raw data into a strategic asset. Information system planning and management involve selecting and implementing the right technology infrastructure for data storage, processing, analysis, and governance. Information technologies and systems play a vital role in facilitating data management within organizations, as they encompass activities such as data acquisition, organization, storage, access, analysis, and interpretation. In the current landscape, characterized by advanced information systems, quick and seamless access to information has become the norm.

There is a distinction between information used for strategic planning and information used for management control. An organization's strategic planning is its process of defining the organization's mission, vision, goals, and objectives, and developing strategies to achieve them, often with the support of information systems, typically done by senior-level managers. In contrast, management control ensures efficient day-to-day operations and adherence to those strategic plans. The information required for each level serves a distinct purpose; hence, the data required also differ. The data need to be in user-friendly formats, enabling managers and analysts to easily comprehend and utilize the information according to their specific requirements (Figure 2.3). Managers, drawing on their expertise and experience while analyzing data, can effectively leverage these insights to address complex business problems. This fosters a dynamic and adaptive approach of leveraging collective data to drive continuous improvement and growth.

Figure 2.3 Data processing for particular purposes generates information, and when applied with business acumen, information creates knowledge. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit Data: modification of work "Project 365 #195: 140709 Let's Get Jiggy With It" by Pete/Flickr, Public Domain; credit Knowledge: modification of work "Thick arrow made from jigsaw puzzle pieces" by Old Photo Profile/Flickr, CC BY 2.0)

Consider an example within the energy sector's need for sustainable energy solutions. To plan information systems for a company in this sector, the chief information officer (CIO) must first understand what decisions need to be made and, correspondingly, what data these decisions require—strategic planning, management control, and operational control. The CIO should assess the different types of data currently available. These data can come from various sources across operations. The focus should be on ensuring existing data capture practices faithfully reflect what's happening in the organization. Additionally, the CIO should consider how these data can be processed and transformed into actionable information that supports the identified decision needs. Finally, the CIO must assess how the different levels of planning and the different types of information fit together.

LINK TO LEARNING

Listen to this podcast about digital transformation at the energy company Shell (https://openstax.org/r/109DigitalTrans) across three levels: operational, management, and strategic.

Frameworks for Data Management Practices and Processes

In the realm of information systems, the Robert Anthony framework, named for the management accounting pioneer who developed it in 1964, helps in understanding information needs across different organizational levels. This framework categorizes decisions based on the level of certainty surrounding the problem and the solution. The **Robert Anthony framework** divides a problem, and by extension the data needed to resolve this problem, into three domains: operational control, management control, and strategic planning[4]:

- Operational control is the process of ensuring that the organization's day-to-day operations are running smoothly. It involves setting production schedules, managing inventory levels, and processing customer orders. Operational control is typically done by frontline managers and employees.
- Management control is the process of ensuring that the organization is meeting its strategic goals. It involves setting budgets, monitoring expenses, and tracking sales. Management control is typically done by middle management.
- Strategic planning is the process of setting long-term goals for an organization. It involves identifying the organization's mission, vision, and values, as well as its strategic objectives. Strategic planning is typically done by the organization's top management team.

By classifying information into these categories, Anthony's framework provides a structured approach to gathering, analyzing, and utilizing information for effective planning and control within an organization. Table 2.1 features data characteristics for the three types of domains.

Domain	Data Use	Data Characteristics
Operational	Track and control day-to-day activities.	Data are typically detailed and time sensitive.
Management	Make decisions about how to allocate resources and achieve goals.	Data are typically summarized and less time sensitive than operational data.
Strategic	Set long-term goals and make strategic decisions.	Data are typically aggregated and less time sensitive than management data.

Table 2.1 Three Domains of the Robert Anthony Framework The three domains of the Robert Anthony framework—operational control, management control, and strategic planning—each work with different types of data for different purposes.

Another data management framework developed by data scientist Herbert A. Simon in 1977, the **decision-making framework** breaks down decisions into two types: programmed decisions with clear procedures or nonprogrammed decisions requiring more judgment. Programmed decisions are also called structured decisions as they are routine and can be made based on preestablished rules and procedures. They often involve repetitive tasks that can be automated within the information system. Nonprogrammed decisions, on the other hand, are not structured as they are unique and complex, requiring judgment, analysis, and creativity. These decisions often arise when there are no predefined guidelines or precedents available. A three-step process determines which activities are programmable and nonprogrammable (Figure 2.4):

1. Intelligence: Gather relevant information and assess the situation to understand the nature and requirements of the activities.
2. Design: Analyze the collected information to make informed judgments about whether an activity can be effectively automated or requires human intervention.
3. Choice: Based on the decisions made, select the appropriate approach for each activity—either programming it for automation or handling it through human involvement.

4 Robert N. Anthony, "Framework for Analysis," *Management Services: A Magazine of Planning, Systems, and Controls* 1, no. 1 (1964): 6, https://egrove.olemiss.edu/mgmtservices/vol1/iss1/6

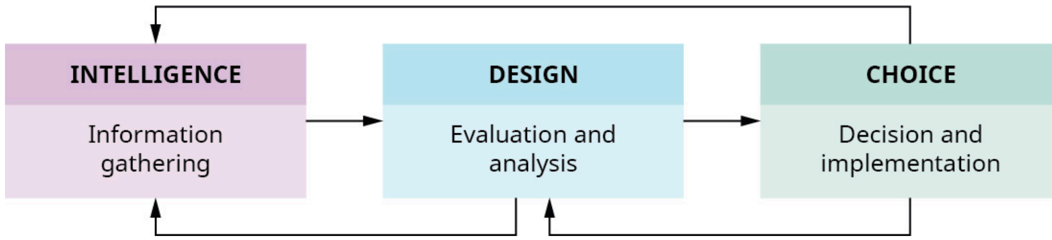


Figure 2.4 To identify whether an activity is programmable or nonprogrammable, a three-step process is followed in order to come to a decision. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Another framework, developed by Gorry and Scott Morton, combines elements of both the Robert Anthony and decision-making frameworks.[5] Gorry and Scott Morton introduced the concept of IT into their framework, acknowledging the influence of technology on decision-making and information management. They highlighted the importance of aligning IT strategic planning with an organization's decision-making needs and the potential benefits that technology can bring to the decision-making process. Gorry and Scott Morton suggest that for each business problem that involves information systems, data managers must first determine whether the problem is strategic, managerial, or operational in nature and then see whether the decision-makers and the intelligence required should be internal or external. If both the decision-makers (stakeholders) and intelligence needed can be found internally, as in the case of order entry and budgeting, then the problem qualifies as being structured. But if both the intelligence needed and the decision-makers are external to the organization, then the problem qualifies as being unstructured, for instance, in the case of systems for cash management or personnel management.

When applying the Gorry and Scott Morton framework to review existing systems or to propose new systems that cater to user needs, an information systems designer or reviewer often investigates how available technology can support decision-making. This framework emphasizes both applications and decisions, necessitating input from a diverse range of users to understand the benefits of existing systems or expectations for new ones. It is important to gather user feedback through structured interviews and questionnaires as they can be utilized to collect user data and gauge user reactions to each system under consideration. Key inquiries may include the following:

- In which directions should the development of new systems be oriented?
- Are there specific demands for enhanced strategic planning applications or managerial and operational systems?
- Do users want a system to support them with decisions that are less structured compared to those handled by existing systems?

Furthermore, an analysis of previous systems developed in analogous situations could offer valuable insights into the potential benefits of a novel system.

5 George A. Gorry and Michael S. Scott Morton, "A Framework for Management Information Systems," *Working Paper No. 510-71*, Alfred P. Sloan School of Management, Massachusetts Institute of Technology, February 1971.

According to the Gorry and Scott Morton framework, management control primarily deals with overseeing and guiding people, while operational control focuses on the performance of designated activities or tasks, such as manufacturing a particular part. Typically, operational control systems have a limited ability to provide managerial control reports or data that are helpful for strategic decision-making. For example, an online retail system primarily focused on operational control can generate sales reports that may provide valuable data for both managerial and strategic decision-making. Similarly, an online retail system primarily focused on operational control can generate reports, such as a sales analysis report. While intended for operational purposes, such reports can also provide valuable data for both managerial and strategic decision-making. For instance, Zara has been able to use online retail system data for its supply chain management system to beat competitors in the time to market by offering new fashions to its customer base.[6] These data can be leveraged to identify sales trends in specific regions, or product categories can inform decisions on marketing expansion, inventory management, and product diversification to drive future growth.

To conduct a thorough examination of the information systems within an organization, a simplified Robert Anthony framework can be employed. First, classify each system requirement based on the user and the type of decision it supports—whether it pertains to operational control, managerial control, or strategic planning. Then, for existing systems, consider factors such as data availability and the governance policies that regulate access by decision-makers. This analysis should help identify whether the existing data align with the intended purpose of the information systems and if any modifications or enhancements are needed. This process may involve reviving outdated systems or proposing new systems.

LINK TO LEARNING

Implementing responsible data management requires an understanding of the legal and social responsibilities associated with processing data across its life cycle.[7] To learn more, read about the Responsible Data Maturity Model (https://openstax.org/r/109RespDataMod) as it recommends how data should be managed to ensure privacy, transparency, sharing, and acquisition of data.

2.2 Strategies to Improve the Value of Information Technology Within Organizations

Learning Objectives

By the end of this section, you will be able to:

- Evaluate and compare different methods to define the value of information technology
- Analyze specific strategies to improve the value of information technology
- Identify real-world strategies organizations use to generate value using information technology

Founded over half a century ago, Domino's Pizza has grown to establish itself as the world's largest pizza company. By 2023, it boasted a global network exceeding 20,000 stores across ninety markets, solidifying its position as a top public restaurant brand. Beyond its impressive scale, Domino's has emerged as a pioneer in leveraging technology to enhance customer experience, developing innovative delivery options like "drop-a-pin" ordering, facilitated by Google Maps Platform mobility services.[8] Domino's adopted NVIDIA's ReOpt tool, a real-time logistics solution that analyzes vast datasets to calculate billions of potential routes, ensuring the fastest and most efficient pizza delivery for each customer.[9] Domino's has quantified the value of their IT investment by measuring improvements in delivery times, a key performance indicator directly linked to customer satisfaction.

6 "Zara Supply Chain Analysis—The Secret Behind Zara's Retail Success," QuickBooks Blog, Intuit Quickbooks, June 25, 2018, https://quickbooks.intuit.com/r/supply-chain/zara-supply-chain-its-secret-to-retail-success/
7 Rashik Parmar, Marc Peters, and Llewellyn D.W. Thomas, "What Is Responsible Computing?" *Harvard Business Review*, July 7, 2023, https://hbr.org/2023/07/what-is-responsible-computing
8 "Domino's: Taking the Guesswork Out of Pizza Delivery with Google Maps Platform," Google Cloud, accessed January 19, 2025,

In today's ever-evolving business landscape, organizations have come to recognize the immense potential of IT to enhance the value of their products and services. Leveraging IT has become a key factor in staying competitive and relevant in the digital age. However, as businesses delve deeper into the realm of IT, they face an essential question: How can they effectively assess the value IT adds to their organization?

Defining the Value of Information Technology Within Organizations

Over the past decades, businesses and managers have focused on understanding how to employ IT systems to achieve goals in diverse organizational, consumer, and societal contexts. Transformative opportunities have been ushered in with the emergence of a new generation of IT, including elements such as:

- crowdsourcing platforms: online marketplaces where businesses or individuals can outsource tasks or problems to a large, dispersed group of people
- cloud computing: on-demand access to computing resources like storage and processing power
- big data infrastructure: systems and technologies needed to manage and analyze massive datasets
- AI: empowering machines to learn and make intelligent decisions
- the Internet of Things: connecting everyday objects to the internet, enabling them to collect and share data

Today's IT systems have evolved and are used in handling tasks that involve high degrees of uncertainty and take place in dynamic and unstructured situations. Some examples of these situations include cars driving autonomously, chatbots supplanting customer service representatives, and email applications suggesting writing improvements. This paradigm shift demands that we explore novel relationships between the strategic value of IT systems and the performance of organizations.

The most common means of understanding the value of information systems in a business is to measure the relationship between IT investments and output measures of revenue and human productivity. This evaluation can be conducted at both the industry level and organizational level. However, the business value of IT goes beyond direct output or revenue measures because IT often supports organizational redesign efforts, such as the traditional taxi services being disrupted by new ride services like Uber or Lyft. This type of business model innovation leverages IT to create entirely new business models, not just enhance existing ones.

Managers should consider which of the following three primary methods of value IT brings to their organization (Figure 2.5):

- automation of operation
- information generation for managing people and resources
- transformation of existing processes or combined tasks called routines

https://cloud.google.com/customers/dominos-maps
9 Jacob Roach, "How Nvidia Is Using A.I. to Help Domino's Deliver Pizzas Faster," *Digital Trends*, November 9, 2021, https://www.digitaltrends.com/computing/nvidia-using-ai-to-help-dominos-deliver-pizzas-faster/

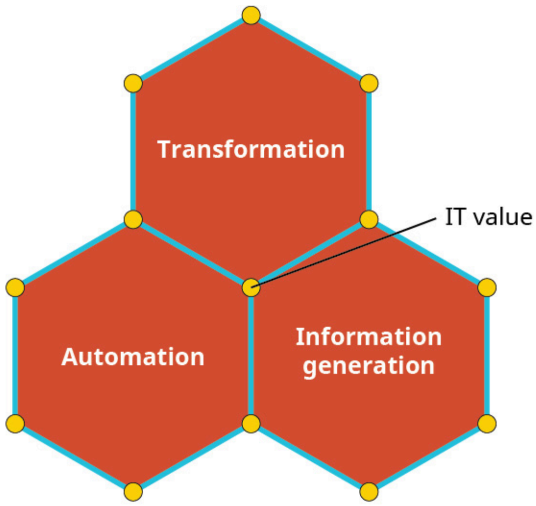


Figure 2.5 Information technology creates value for organizations through automation, information generation, and transformation. (credit: modification of work “Tiling 6 simple” by T. Piesk/Wikimedia Commons, CC BY 4.0)

The automation of repetitive and mundane tasks via IT enables organizations to increase efficiency and reduce human error. For example, automating inventory management processes can streamline supply chain operations, leading to cost savings and improved inventory control. Automation can also enhance customer service through the deployment of chatbots or virtual assistants that can handle routine inquiries and thereby free up human agents to focus on more complex customer needs. For instance, Domino’s leverages IT to automate tasks associated with delivery route planning, finding the most efficient delivery routes, reducing the need for manual planning, and saving valuable time for employees.

Information generation through IT can also empower organizations to make strategic choices based on real-time and accurate data, which can lead to better decision-making and increased competitiveness. Information technology systems capture vast amounts of data from various sources, including customer interactions, market trends, and internal operations. Through advanced data analytics and business intelligence tools, organizations can derive valuable insights and make data-driven decisions. For instance, understanding customer preferences based on data analysis allows businesses to tailor their products and services to meet specific demands, improving customer satisfaction and loyalty. Domino’s utilizes various IT systems to generate real-time data on traffic conditions, delivery times, and customer locations. By analyzing this data, Domino’s gains valuable insights that inform decision-making. For instance, they can identify areas for improvement in delivery routes or optimize staffing levels based on anticipated demand.

Through IT, organizations can transform and reimagine their products, services, and customer experiences. The rise of e-commerce transformed the retail industry, allowing companies to reach an international audience and provide personalized shopping experiences. Embracing cloud computing, AI, and data analytics can lead to innovation and new revenue streams, ultimately enhancing an organization’s overall value proposition. For example, Under Armour attempted to transform itself from a sports apparel brand into a holistic fitness and wellness company through the acquisition of MyFitnessPal and the development of its own fitness app. It planned for IT and its management to leverage data and technology to move beyond selling clothes and become a central hub for athletes and fitness enthusiasts.[10]

LINK TO LEARNING

Read more about Under Armour’s transformation strategy (https://openstax.org/r/109UnderArmour) and learn how it fared (https://openstax.org/r/109UASuccess) and how the company adapted their strategy

10 Parmy Olson, “Under Armour Buys Health-Tracking App MyFitnessPal for $475 Million,” *Forbes*, February 4, 2015, https://www.forbes.com/sites/parmyolson/2015/02/04/myfitnesspal-acquisition-under-armour/

moving forward.

An individual department or functional area within a large organization may have its own specific IT application program known as a **functional area information system (FAIS)**, an information system designed to support specific business functions within the organization. These FAISs are designed to enhance the internal efficiency and effectiveness of each department by providing valuable support tailored to each respective department's functions. These information systems often generate a diverse range of reports. Some common examples of functional areas for FAIS include accounting, finance, production and operations management, marketing, and human resources. The indicators of value listed in Table 2.2 signify the positive outcomes and advantages that result from investing in IT within each functional area and system category.

Functional Area	Strategic Information Systems	Managerial Information Systems	Operational Information Systems	Overall Value Indicators for Information Technology Investment
Human resources	Workforce optimization	Data-driven human resources decision-making and analytics	Efficient employee data management and self-service options	Improved talent acquisition and retention, reduced human resources operational costs
Finance and accounting	Effectiveness of real-time financial insights and predictive analysis	Streamlined budgeting and financial forecasting	Automated accounting processes and payroll management	Better financial decision-making, cost savings, minimized errors
Sales and marketing	Acquisition and retention of customer with data analysis for market trends and demand forecasting	Sales performance tracking and sales pipeline management	Target marketing campaigns and customer engagement	Increased sales, enhanced customer satisfaction, improved marketing return on investment
Manufacturing and operations	Product life-cycle optimization and risk assessment	Efficient materials and production planning	Real-time shop floor monitoring and quality control	Improved product quality, reduced production downtime, streamlined processes
Supply chain management	Supply chain visibility and demand forecasting	Inventory optimization and supplier performance tracking	Efficient order processing and shipment tracking	Reduced inventory costs, improved supply chain efficiency

Table 2.2 FAIS Values These indicators serve as metrics for evaluating information technology investments and demonstrate how technology can create value for organizations.

Functional Area	Strategic Information Systems	Managerial Information Systems	Operational Information Systems	Overall Value Indicators for Information Technology Investment
Customer service	Acquisition and retention of customers; customer feedback and sentiment analysis	Help desk performance analytics and ticket tracking	Customer self-help knowledge base and issue resolution	Enhanced customer satisfaction, reduced response time, and support costs
Research and development	Rate of collaborative innovation and new idea generation	Project resource allocation and innovation tracking	Idea evaluation and research and development process optimization	Accelerated innovation, streamlined research and development processes, and successful product development
Information technology and technology management	Alignment of information technology investments with business goals and strategy	Information technology project progress monitoring and resource optimization	Efficient information technology service delivery and asset management	Optimized information technology spending, improved project outcomes, and reduced operational disruptions
Business intelligence and analytics	Utilization of data for advanced analytics	Data visualization for insights and decision-making	Interactive dashboards for real-time performance tracking	Data-driven decision-making, actionable insights, and improved business performance

Table 2.2 FAIS Values These indicators serve as metrics for evaluating information technology investments and demonstrate how technology can create value for organizations.

Strategies to Improve the Value of Information Technology for Organizations

Understanding the role of business processes within an organization is vital to measuring the specific value that IT can deliver and the mechanisms through which it achieves this. Information systems professionals know that technology alone is not the sole determinant of digital success, and that strategy is an important catalyst in the digital domain. Business-IT alignment, or strategic alignment, refers to the strong integration of the IT function with an organization's strategy, mission, and objectives. This simply means that IT directly supports the business goals of the organization. Successful alignment exhibits six key characteristics (Figure 2.6):

- Organizations consider IT to be a driver of innovation that continuously transforms the business, leading to new revenue opportunities.
- Internal and external customers, as well as customer service, hold paramount importance for these organizations.
- Business and IT professionals are cross-trained and move across different departments and job roles.

- Clear overarching goals are established and understood by both IT and business employees.
- Information technology employees are informed about the company's revenue generation and cost-saving mechanisms.
- The organization fosters a vibrant and inclusive company culture.

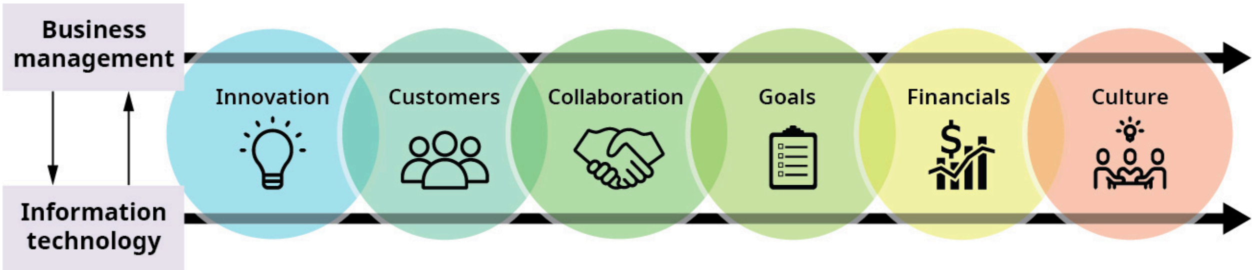


Figure 2.6 Successful strategic alignment occurs when information technology directly supports the business goals of the organization, guided by these six characteristics. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit Innovation: modification of work "Idea (89054) - The Noun Project" by "Nice and Serious"/Wikimedia Commons, CC0 1.0; credit Customers: modification of work "Noun Project people icon 3376085" by Anhar Ismail, ID/Wikimedia Commons, CC BY 3.0; credit Collaboration: modification of work "Handshake, by David" by David/Wikimedia Commons, CC BY 3.0; credit Goals: modification of work "Checklist Noun project 5166" by Aaron Dodson/Wikimedia Commons, CC BY 3.0; credit Financials: modification of work "Analysis (1510724) - The Noun Project" by Anwer Hossain/Wikimedia Commons, CC0 1.0; credit Culture: modification of work "Ethics of Open Sharing icon - Organizational culture" by Julius Uusikylä, KRUT Collective/Wikimedia Commons, CC0 1.0)

Unfortunately, many organizations struggle to achieve such close alignment. The primary reasons for the gap between business and IT departments can usually be attributed to the following:

- Different objectives: Business managers focus on achieving business goals and generating revenue, while IT managers concentrate on technology implementation and maintenance.
- Lack of expertise awareness: Business and IT departments often lack awareness of each other's expertise and perspectives, leading to misunderstandings and misalignment.
- Lack of communication: Inadequate communication between business and IT executives hinders the exchange of valuable insights and requirements.

Business and IT alignment as an integral unit, not separate entities, is vital. It is important that organizations view IT as a strategic partner, not just a support function. By fostering collaboration and communication between business and IT stakeholders, organizations can ensure that technology solutions directly address business needs and objectives. To improve business-IT alignment, organizations can employ several measures:[11]

- Prioritize organizational communication: Encouraging effective dialogue between different departments, fostering interdepartmental partnerships, and promoting mutual understanding between business and IT teams ensures sufficient knowledge sharing, well-informed decision-making, and seamless collaboration.
- Focus on strengthening governance: Organizations should involve IT in strategic planning to ensure technology initiatives align with overall business goals. Engaging IT in executive committees enhances the decision-making process. Implementing a structured reporting hierarchy establishes clear communication channels, and defining authorization for decision-making roles ensures efficient execution. Coordinated governance can help set criteria whereby IT projects are prioritized based on their alignment with business objectives.
- Align scope and IT architecture: Evaluating IT solutions for their effectiveness and customizing them to suit specific scope and business needs can lead to better outcomes.
- Emphasize the development of human skills: Cultivating readiness to embrace technological changes, adapting management styles to support successful IT implementation, and learning from previous experiences contribute to continuous improvement.

11 Sahar Alsharif, Nabila Benslimane, Mohamed Khalifa, and Colin Price, "Healthcare IT Strategic Alignment: Challenges and Recommendations," *Studies in Health Technology and Informatics* 251 (2018): 207–210, https://doi.org/10.3233/978-1-61499-880-8-207

Case Study: High-Tech Stumble of UK Identity Cards

In the early 2000s, the UK government aimed to enhance national security, combat identity fraud, and improve public services through the introduction of a comprehensive identity card. These cards would store biometric data and personal details, providing a centralized system for identification. However, the plan faced fierce opposition from civil liberties groups, privacy advocates, and political parties. Critics argued that the identity cards would compromise individual privacy rights and lead to excessive surveillance of citizens. Concerns were raised about data misuse, potential breaches, and the vulnerability of a centralized database to hacking. Despite efforts to emphasize the benefits of the identity cards, the opposition prevailed, and the proposal was eventually abandoned. The incoming coalition government decided that the proposal was too costly and lacked significant advantages for national security, underscoring the misalignment between business and IT strategies. Although the national identity card plan was discontinued, specific ID cards, like the biometric residence permit for non–European Union nationals, were introduced as documentation of a person's immigration status.

The details of this case reveal a significant misalignment between IT and business perspectives concerning the technological aspect of identity cards. Overall, the disparity between the UK's simple, traditional ID cards and the envisioned technological sophistication of the new cards highlighted the disconnect between IT and business perspectives: the clash between a simple, efficient approach and the pursuit of advanced technology. This case emphasizes the importance of fostering collaboration and understanding between IT and stakeholders to develop practical and effective solutions for many different business scenarios.

Strategies to Generate Value Using Information Technology

In today's business landscape, there are five key strategies usually pursued by organizations when seeking to generate value using IT: cost leadership, differentiation, focus/innovation, operational effectiveness, and customer orientation.

Cost leadership strategy is a business approach wherein a company aims to become the lowest-cost producer in its industry or market. The primary goal of this strategy is to offer products or services at the lowest possible price while maintaining acceptable quality levels. Walmart's focus on cost leadership has allowed it to maintain a dominant position in the retail industry. It consistently outperforms competitors by offering lower prices and attracting a broad customer base, including price-sensitive shoppers. Despite its low-margin business, Walmart's sheer scale and operational efficiency allow it to generate massive revenue while maintaining profitability.

Differentiation strategy is a business approach wherein a company seeks to distinguish its products or services from those of its competitors in the industry. The primary goal of this strategy is to create a unique and desirable offering that customers perceive as superior and are willing to pay a premium for. Apple exemplifies the differentiation strategy in the marketplace. By designing sleek and user-friendly products, Apple sets itself apart from competitors. The company's focus on design, seamless integration of hardware and software, and emphasis on creating a unique user experience differentiates its products in the market.

Focus/innovation strategy is a business approach wherein a company focuses on introducing new products, services, or processes—or enhancing existing ones—to stay ahead of the competition and meet evolving customer needs. The primary goal of this strategy is to drive growth and create a competitive advantage by being at the forefront of innovation in the industry. Google is a prime example. Continuously introducing new products and features, such as Google Search, Gmail, and Google Maps, the company revolutionized the way people access and interact with information online.

Operational effectiveness strategy is a business approach wherein a company focuses on improving the efficiency and effectiveness of its internal business processes to outperform competitors. The primary goal of this strategy is to achieve higher productivity, quality, and customer satisfaction while reducing operational costs and time to market. Amazon's success is attributed to its operational effectiveness strategy. By optimizing its e-commerce platform, warehouse management, and delivery network, Amazon ensures efficient order processing and swift delivery of products to customers.

Customer-oriented strategy is a business approach wherein a company places a strong emphasis on understanding and meeting the needs, preferences, and expectations of its customers. Also known as the customer-centric strategy, the primary goal of this strategy is to build long-lasting and loyal customer relationships by providing personalized and exceptional experiences. Netflix thrives on a customer-oriented strategy. Utilizing sophisticated algorithms and user data, Netflix offers personalized content recommendations to each subscriber, tailoring their streaming experience based on their individual preferences.

Each of these strategies has its pros and cons. For example, if a company focuses only on pursuing a cost leadership strategy, it might not have enough resources for research and development, and so it might lag in terms of innovation. Let's say a company traditionally sells a one-size-fits-all software product, and they decide to shift toward a customer-oriented strategy by offering customizable features and personalized support options. A customer-oriented strategy impacts the scope, cost, schedule, risk, and quality dimensions of a project. While a customer-oriented approach can lead to higher initial costs, it can also bring significant benefits.

2.3 Digital Business Models

Learning Objectives

By the end of this section, you will be able to:

- Compare digital business models and their design and integration components
- Critique digital business models

The use of IT offers businesses numerous opportunities to generate value. Since most businesses adopt IT, undergo digital transformation, or fundamentally change how the business operates and delivers value using digital technologies, the digital field is crowded with apps, services, platforms, and digital devices. Some businesses undergoing digital transformations thrive initially but then go bankrupt, and others pivot and survive. Many established companies like retailers, banks, travel agencies, and print media have struggled to survive in the face of digital disruption. Organizations confront a common challenge—the necessity to develop digital business models that deliver value to customers or users. Thus, business models act as the vital connector between technology and the strategic goals of an organization (Figure 2.7).

Figure 2.7 The business model is the key to bridging the gap between technological potential and business success, paving the way for companies to thrive in the competitive landscape. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit gears: modification of work "Noun project 1063" by Jeremy Minnick/Wikimedia Commons, CC0 1.0; credit people with laptops: modification of work "Noun project - Meeting with laptops" by Slava Strizh/Wikimedia Commons, CC BY 3.0; credit target: modification of work "Noun 108494 cc" by Dima Lagunov/Wikimedia Commons, CC BY 3.0)

Defining Digital Business Models

A successful digital business model provides a logical framework that unlocks the value of a technology, allowing businesses to benefit economically. The business model serves as a blueprint for how a company generates and captures value from new products, services, or innovations. It is not solely IT that determines success, but the business model behind it that plays a key role in enabling high-tech companies to achieve their strategic goals and objectives. There are several common digital business models, each of which has specific information technology strategies.

The **e-commerce model** involves buying and selling goods or services online through websites or apps, and offers convenient shopping experience for various customer segments. Notable examples of companies using this model are Amazon, Alibaba, and Shopify. In terms of IT strategy, a company using this model should develop robust and secure e-commerce platforms to align with business objectives, such as providing a seamless customer journey, implementing secure payment gateways, and optimizing logistics for efficient order fulfillment. The organization should also align IT with marketing strategies to enable personalized product recommendations and targeted promotions, ultimately driving customer engagement and loyalty.

The **subscription model** provides continuous value through recurring subscriptions that provide customers with ongoing premium content or services. The IT strategy for this model is to develop products and/or services, such as entertainment and transportation, that customers need routinely and are willing to make recurring payments for to have continued access to the products and/or services. Amazon Prime and YouTube are subscription models.

The **freemium model** provides a free basic service, with the option to upgrade to a premium version for enhanced features or benefits, such as with the services offered by LinkedIn, DropBox, and MailChimp. Integrating IT should involve designing services that showcase the value of the basic offering to entice users to upgrade to premium features, such as a seamless onboarding process and data-driven user engagement tactics. Companies should also optimize the platform to manage both free and paying users effectively. Effective data analytics and user segmentation are necessary to identify potential premium users. Collaboration with marketing and sales teams can be used to design targeted conversion strategies, monitor user behavior to optimize premium feature adoption, and continuously improve the platform to increase conversion rates and drive revenue growth.

In an **affiliate model**, one company earns commissions by promoting and selling other companies' products or services through websites or social media channels. They help drive traffic and sales, receiving a percentage of the revenue from the companies they promote. Amazon Associates, ClickBank, and Commission Junction use this model. These organizations should work with IT to build effective tracking and reporting systems to accurately attribute sales to affiliates by implementing affiliate tracking software, optimizing landing pages for conversion, and ensuring a seamless user journey from the affiliate's site to the merchant's platform. Providing real-time data and performance insights to affiliates enables them to optimize their promotional strategies.

Amazon, eBay, and Airbnb demonstrate the **marketplace model**, which brings buyers and sellers together on a single platform, with the enterprise acting as an intermediary that facilitates transactions between parties. This approach fosters a diverse range of goods and services offered by different sellers, making it a convenient hub for buyers. Effective IT strategy for this digital business model includes providing efficient search and filtering options for users, securing payment gateways, personalizing recommendations, and offering robust customer support systems that ensure smooth transactions and build trust between buyers and sellers. Organizations using this model should also enable a user-friendly interface, smooth transaction processes, and personalized product recommendations based on user behavior and preferences.

The **advertising model** generates revenue through targeted ads purchased by other businesses. Ads are presented to customers when they view content, and since the content is supported by advertising revenue paid by other businesses, customers view the content free of charge. This is the model for Facebook and PeopleFun. IT strategy for this approach includes developing content that includes space for advertisements that can be presented to users as they browse content, and selling this space to other businesses to run their ads for an allotted time, based on the fees paid for the ads. Ads should be programmed and presented to attract users' attention while also providing minimal disruption to users' interaction with content.

Kickstarter, Indiegogo, and GoFundMe operate through a **crowdfunding model**, which raises funds for a product, project, or idea through an online platform, leveraging the collective support of the public. In this scenario, contributors pledge funds to support initiatives and receive rewards or early access to products in return. Entities utilizing this model should ensure their IT strategy is designed to build secure payment gateways, provide real-time updates on fundraising progress, offer personalized backer rewards, and implement social sharing features to enhance campaign visibility and engagement. They should also ensure a user-friendly platform for both project creators and contributors, enabling easy navigation and smooth communication channels.

A **sharing economy model** involves individuals sharing resources or services through a peer-to-peer network, enabling efficient utilization of underused assets. This fosters collaboration and convenience among users seeking specific services or goods. Uber, Airbnb, and TaskRabbit are examples of companies using this model. In terms of IT strategy, those with a sharing economy model should build robust peer-to-peer communication systems that implement secure payment processing, real-time tracking features, and rating and review systems to build trust among users. It is also important to prioritize user safety and enable efficient communication between providers and consumers.

Finally, the **digital product model** offers downloadable digital assets that may include actual products, such as e-books, or may be used to provide information such as education, assembly instructions, or details about a product's components. The offerings seen from TurboTax and Apple's iTunes Store are digital products that are downloaded. IT strategy focuses on developing products and services that can be delivered and used in an electronic format. Companies should provide customers with a seamless process that enables them to download products, such as software or music, or access services, such as an online class, on any device, including computers, tablets, and cell phones. They should also enable real-time access, provide prompt user support, and implement security protocols that ensure user safety when users download material or interact online.

Today's business environment has undergone significant transformations. Unlike the traditional stable and low-competition business world, the digital business realm is marked by complexity, dynamism, and high levels of uncertainty and competition. Consequently, in this intricate digital business setting, the business model must be explicit and highly flexible to adapt effectively. Embracing change is important for effectively navigating today's business landscape.

LINK TO LEARNING

Learn about AI-generated music (https://openstax.org/r/109AIMusic) and how AI is disrupting the music industry as well as freemium and subscription business models.

Case Study: Transforming Health Care Through the Sharing Economy Model

The U.S. health-care industry faces a substantial inefficiency issue, with a large portion of capital expenditure going toward medical equipment that remains underutilized. Boston-based Cohealo recognized the potential of the sharing economy model to address these inefficiencies and created a platform that facilitates the seamless sharing of medical equipment across different facilities. Cohealo operates as a cloud-based platform supporting logistic capabilities and as an analytics-enabled information system that enables customers to manage medical equipment centrally and make it available on demand. Cohealo's products include the following:

1. Cohealo + C-suite: This product functions as a comprehensive customer relationship management platform, allowing hospital management to access and manage equipment-related data. The platform offers real-time data and usage analytics, centralized decision-making, and personalized dashboards, enabling clinics to optimize resource deployment effectively.
2. Cohealo + Finance: Clinics can make data-driven capital decisions in real time with this tool, optimizing the utilization of their most critical technology investments. By spreading out costs and consumption, Cohealo enables new efficiencies, faster capital redeployment cycles, and improved return on investment.
3. Cohealo + Clinical: This network-based application empowers clinics to locate and enlist any idle medical

equipment across the network to support procedures wherever and whenever needed. This manufacturer-agnostic design puts the choice in the hands of clinics, freeing up administrative time for patient and physician care.

4. Cohealo + Supply Chain: Cohealo streamlines equipment transportation, ensuring it reaches the required location optimally and returns to the original site after usage. The network effect, fostered by health-care institutions clustered in and around Boston, contributes to the success of Cohealo's platform, enabling the emergence of disruptive business models.

Several factors influence the success of the sharing economy model in the health-care sector, as observed in Cohealo's case[12]:

- Resource characteristics: Medical equipment, being valuable and commercial in nature, is considered suitable for sharing.
- Clustering of resources: The concentration of interconnected health-care companies and institutions in specific geographic locations facilitates the easy transfer of use rights.
- Use of IT: Online platforms enable easy and efficient mediation and monitoring of contract terms.
- Cost advantage: The cost of accessing shared resources through Cohealo is often significantly lower than the cost of ownership, promoting the adoption of the sharing economy model.
- Institutional support: Factors like supply chain and logistics support, as well as governance considerations, enhance the feasibility of sharing resources within the health-care industry.[13]

Digital Business Model Critiques

The emergence of digital business models has created the space for a workforce through online platform–based work. While this has brought about innovative solutions for economic interactions between people seeking jobs and employers, it has opened new challenges. With the sharing economy business model, algorithmic reputation features play a central role in fostering trust and accountability. These reputation systems, based on customer feedback and ratings, have been hailed as a valuable trust mechanism resulting in efficient matches for a distributed workforce. Some criticism and challenges faced by digital business models include[14]:

- Unequal distribution of opportunities: Research has shed light on a concerning phenomenon observed in gig work platforms—the "rich get richer" effect. Workers with higher reputation scores and greater experience tend to receive more work, as clients prefer to engage with those perceived as more reliable. Consequently, this phenomenon results in an unequal distribution of opportunities, disadvantaging workers with lower scores and less experience.
- System of control: Algorithmic systems, though designed to foster trust, inadvertently create a "system of control." By standardizing metrics and homogenizing worker identities, platforms such as Uber or DoorDash wield significant power. Platforms can manipulate scoring and matching algorithms to influence job allocation decisions without involving the people using their platforms.
- Opacity and lack of transparency: One of the most troubling aspects of algorithmic digital systems is their opacity. Proprietary algorithms protected by trade secrecy laws prevent external scrutiny, leaving users in the dark about the factors influencing their reputation scores or how changes to algorithms may impact their job opportunities. In digital platforms such as Upwork, there is electronic monitoring of user actions that affects their perceived autonomy.[15]

12 Ayushi Tandon, "Cohealo! Sharing Economy Determinants in Healthcare Industry," *SSRN*, December 2017, http://dx.doi.org/10.2139/ssrn.3677462

13 Vijaya Sunder M and Sowmya Shashidhara, "Next Step in Healthcare: Sharing Economy to Overcome Resource Crisis," *Forbes India*, October 8, 2021, https://www.forbesindia.com/article/isbinsight/next-step-in-healthcare-sharing-economy-to-overcome-resource-crisis/70893/1

14 Zhi Ming Tan, Nikita Aggarwal, Josh Cowls, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi, "The Ethical Debate About the Gig Economy: A Review and Critical Analysis," *Technology in Society* 65 (May 2021): 101594, https://doi.org/10.1016/j.techsoc.2021.101594

15 Kristine M. Kuhn and Amir Maleki, "Micro-Entrepreneurs, Dependent Contractors, and Instaserfs: Understanding Online Labor Platform Workforces," *Academy of Management Perspectives* 31, no. 3 (2017): 183–200, https://doi.org/10.5465/amp.2015.0111

ETHICS IN IS

IBM's Artificial Intelligence Ethics Initiatives

IBM provides a notable example of IS ethics in AI decision-making. IBM has been actively working on ethical AI initiatives, emphasizing fairness, transparency, and accountability in algorithmic decision-making across various domains such as hiring, lending, and law enforcement. IBM's approach involves developing AI systems that mitigate biases, ensuring inclusivity, and safeguarding privacy through responsible data practices. Their efforts include implementing ethical AI frameworks, promoting diverse datasets, and advocating for AI transparency and explainability to address societal concerns regarding algorithmic fairness and discrimination.[16]

2.4 Business Process Management

Learning Objectives

By the end of this section, you will be able to:

- Describe a business process
- Differentiate business process reengineering, improvement, and management
- Discuss ways in which information systems enable business processes

To promote success, businesses and other organizations need robust business processes that are well managed. Business processes help organizations be more efficient and effective—providing higher-quality products and services, and improving customer service and satisfaction. Business processes can be tailored to meet an organization's specific needs, and information systems can be important tools to enhance business processes.

Business Process

A **business process** represents a continuous series of interconnected activities aimed at producing a valuable product or service for an organization, its business partners, and its customers. This process relies on three essential components:

- Inputs: These encompass the materials, services, and information that flow through the process and undergo transformations as a consequence of the activities within the process.
- Resources: People and other resources form the backbone of process activities, performing various tasks to facilitate the progression of the process.
- Outputs: Outputs are the ultimate result of the process, ending in the creation of a specific product or service that is ready to be delivered to the intended recipient.

Consider the design of an information system for booking a COVID-19/flu/RSV test online. As shown in Figure 2.8, this business process includes procedures such as user registration, test availability search, appointment booking, secure payment, test result reporting, and verification. The information system may prioritize data privacy and offer reliable customer support to enhance user experience. Regular updates and maintenance ensure efficiency and compliance with evolving guidelines. In general, efficient and well-designed business processes are crucial for gaining a competitive advantage and ensuring organizational success. Such processes must enable the information system to function innovatively and with enhanced effectiveness and efficiency compared to its competitors. Conversely, poorly designed processes could become liabilities, hindering the information system's responsiveness and productivity.

16 "What Is AI Ethics," IBM, September 17, 2024, https://www.ibm.com/topics/ai-ethics

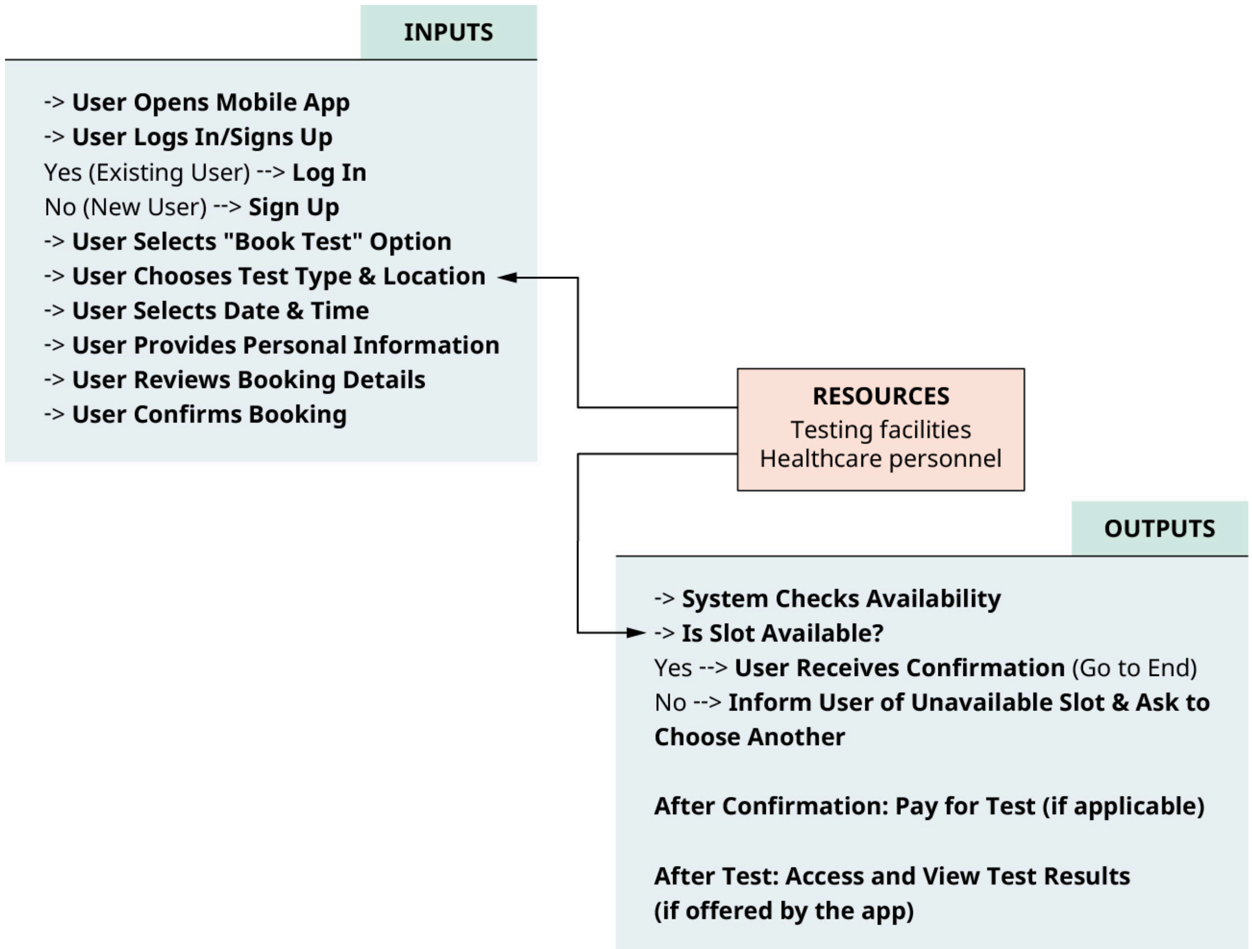


Figure 2.8 Consider an example of booking a COVID-19/flu/RSV lab test through a mobile app. The inputs required from users are personal information and preferred testing locations, and the outputs generated are confirmation of booked slot and test details. Additionally, it involves identifying the resources needed, which in this case are testing facilities and health-care personnel, to ensure a smooth and seamless process. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Providing an easy-to-use, up-to-date information system that delivers swift responses to user queries is essential for attracting customers and increasing usage. Accuracy in displaying current information related, in this case, to available time slots, testing locations, and pricing is crucial to building trust and reliability among users. Conversely, an information system that fails to offer timely and accurate information or has slow response times can have adverse effects on its success and reputation.

To assess whether the business processes of an information system are well designed, the first step is to document the entire process. By analyzing this process, the organization behind the information system can identify potential areas for improvement to gain **competitive advantage**, which refers to conditions and circumstances that enable a company to compete more effectively than its rivals in a given market. A competitive advantage helps an organization control a market and accrue profits.

Business Process Reengineering, Improvement, and Management

Table 2.3 identifies fundamental business processes performed in an organization’s functional areas. However, there are several other business processes, such as procurement and fulfillment, that span multiple functional areas. These processes are referred to as cross-functional business processes, where no single functional area solely bears the responsibility for their execution. To ensure the successful completion of a cross-functional process, each functional area involved must execute its specific steps in a well-coordinated and collaborative manner.

Functional Area	Business Process Examples
Accounting	• Processing vendor invoices and managing accounts payable • Handling customer invoicing and managing accounts receivable • Conducting bank account reconciliations for financial accuracy • Managing cash receipts and maintaining proper records • Preparing financial statements for reporting and analysis • Managing payroll and employee compensation
Finance	• Collecting outstanding payments from customers • Facilitating and processing bank loan applications • Generating business forecasts for financial planning • Conducting customer credit approval and setting credit terms • Managing investment portfolios and analyzing returns • Evaluating and negotiating financial contracts • Budgeting and controlling expenses
Marketing	• Engaging in postsale customer follow-up activities • Conducting customer satisfaction surveys to gather feedback • Developing marketing campaigns and strategies • Managing social media presence and online advertising • Analyzing market trends and competitor research • Launching new products and services
Production/operations	• Managing bills of materials for production processes • Processing manufacturing change orders for product improvements • Handling packing, storage, and distribution of finished goods • Conducting physical inventory checks for accurate stock levels • Overseeing quality control processes for finished products • Implementing lean manufacturing principles for efficiency • Managing supplier relationships and inventory procurement

Table 2.3 Business Process of Different Functional Areas There are numerous fundamental business processes performed across an organization’s functional areas.

Functional Area	Business Process Examples
Human resources	• Administering HR policies and providing necessary support • Managing employee hiring and conducting orientation programs • Maintaining employee files and records for documentation • Handling health-care benefits and ensuring employee well-being • Managing performance appraisals and salary adjustments • Conducting employee training and development programs • Implementing workplace policies and compliance
Management information systems	• Implementing antivirus control measures for data security • Reporting and addressing computer security incidents • Conducting computer user training for efficient system usage • Applying disaster recovery procedures for data protection • Developing and implementing policies for email and internet use • Managing information technology infrastructure and system maintenance • Analyzing and improving business processes through technology

Table 2.3 Business Process of Different Functional Areas There are numerous fundamental business processes performed across an organization's functional areas.

Organizations document any business process, and if any inefficiencies or bottlenecks are detected, modifications can be made to optimize the platform's performance and enhance user experience. In the COVID-19 test booking example, modifications may include streamlining the booking flow, optimizing the database for faster information retrieval, and ensuring the platform's scalability to handle increased demand during peak times. This is much like the e-ticketing process used in the airline industry. Here are some key measures of excellence when evaluating the execution of a business process:

- User satisfaction: Efficient and well-designed business processes can contribute to a more positive work environment, leading to higher satisfaction and engagement of those using these processes.
- Innovation: Streamlined processes can free up resources and time, allowing organizations to invest more in research and development, leading to greater innovation.
- Flexibility and adaptability: Agile and adaptable business processes enable organizations to respond quickly to changes in the market or industry, enhancing their ability to stay relevant and competitive.
- Cost reduction: By optimizing operational procedures and supplier processes, organizations can achieve cost-cutting objectives, leading to improved financial efficiency.
- Quality: The optimization of design, development, and production processes results in the delivery of superior-quality products or services, which builds a reputation for excellence.
- Differentiation: By optimizing marketing and innovation processes, organizations can create unique and distinctive offerings that set them apart from competitors and help them establish a competitive edge.
- Customer satisfaction: Attaining strong customer contentment is a direct outcome of streamlining and harmonizing business processes to effectively meet the needs and preferences of customers.
- Environmental impact: Optimized processes can lead to reduced waste and resource consumption, positively impacting the organization's environmental footprint.
- Compliance and governance: Well-structured processes can ensure that the organization complies with relevant regulations and governance standards, thereby reducing its legal and reputational risks.

How does an organization ensure business process excellence? One approach developed in the 1990s is **business process reengineering (BPR)**, which describes the radical rebuilding of core business processes to achieve optimization. This strategic approach strives to expand the productivity and profitability of an organization's business processes. In essence, BPR requires organizations to scrutinize their business processes through an unprejudiced lens and subsequently determine the optimal means to reconstruct these processes to bolster their business functions. Business process reengineering originates from the capabilities IT offers, including process automation, standardization of several process steps, and error mitigation through improved interdepartmental communication.

Although some enterprises have effectively implemented BPR, a significant number of organizations found this strategy to be excessively intricate and challenging to pursue. After encountering setbacks in BPR implementation, businesses increasingly shifted their focus toward organizing work around business processes rather than individual tasks. This shift led to a less disruptive and more gradual approach known as **business process improvement (BPI)**, which is the valuation of existing business processes to identify areas for improvement. For instance, if a social media marketing platform were to experience a decline in click-through rate (CTR), a metric that measures the effectiveness of an online ad or link, the organization's BPI team would investigate the root cause behind this issue. Likewise, if there was a broken machine on an assembly line leading to output variations, the BPI team would analyze the process to rectify the problem. The BPI team is composed of individuals with various roles and expertise. It typically includes the process owner, process experts, subject matter experts, data analysts, and cross-functional representatives from different departments. Continuous improvement specialists may also be part of the team, and a project manager or facilitator leads the efforts. Stakeholders, including customers or end users, may also be involved or consulted for their valuable input.

For example, consider a social media marketing platform that developed a campaign promoting a new product launch. The initial CTR was 3.5 percent, and the marketing team aspired to improve this metric. By using the BPI methodology, the team investigated the possible reasons for the low CTR. On analysis, it found that the ads lacked visual appeal and failed to communicate the product's unique selling points effectively. Additionally, the team discovered that the targeting parameters needed refinement, as the ads were reaching an audience that was not very likely to be interested in the product. Based on these insights, the marketing team implemented the following improvements:

- Ad creative enhancement: The BPI team collaborated with a creative team to design visually captivating and compelling ad content that better communicated the product's features and benefits.
- Targeting refinement: The team revised the audience targeting parameters, focusing on demographics and interests more closely aligned with the product's target market.
- A/B testing: To gauge the effectiveness of the changes, the team conducted A/B testing with different versions of the ad, comparing their performances to determine which ones yield better results. An A/B test compares the performance of two versions of content to see which one appeals more to viewers.

In addition to A/B testing, two popular methodologies used in BPI initiatives are design thinking and Agile. As a methodology, **design thinking**, which is an approach to problem solving that uses creativity and empathy to understand user needs in order to create user-centric products and services, has roots in the field of design and was popularized in the 1990s by companies such as IDEO. The methodology involves empathizing with customers to understand their pain points, defining the problem clearly, generating possible solutions, prototyping and testing these solutions, and finally, implementing the most effective ones. For instance, a financial institution may use design thinking to enhance its customer onboarding process. By integrating the human-centered approach of design thinking, organizations can create processes that resonate with their customers, improve user experience, and drive better business outcomes. The Agile methodology, as you've learned, is used in software development and other fields, particularly for projects with rapidly changing requirements and a need for frequent iterations, that emphasize flexibility, iterative development, and collaboration. For example, a software development team working on a mobile application might employ Agile to deliver incremental updates and new features in short development cycles (sprints). This iterative approach allows the team to gather continuous feedback from users and stakeholders, ensuring that the final product meets their evolving needs.

To sustain BPI efforts over time, organizations can adopt **business process management (BPM)**, which is the ongoing review and analysis of processes across an organization to identify opportunities for improvements or reengineering that will optimize core business processes. BPM relies heavily on process modeling to show stakeholders the dependencies between the people, systems, and information that interact to perform tasks successfully. Along with business activity monitoring, this approach strives to make BPI initiatives more congruent through optimization of core business processes.

Business process management begins with process modeling, which is a graphical depiction of all steps in a process. Process modeling helps employees understand the interactions and dependencies among the people involved in a given process, the information systems they rely on, and the information they require to optimally perform their tasks. Business process management involves several key parameters that contribute to the successful digitalization of business process initiatives within an organization:[17]

- Strategic alignment: Business process management must be closely aligned with the organization's overall strategy. This alignment ensures that processes are designed, executed, managed, and measured in accordance with strategic priorities, enabling continuous and effective actions to improve performances of specific business processes. Business models act as the vital connector between the technology strategy and strategic goals of an organization.
- Methods: Business process management methods consist of tools and techniques supporting activities throughout the process life cycle and enterprise-wide BPM initiatives. Examples include process modeling, analysis, and improvement techniques with approaches like design thinking and Six Sigma, a quality management methodology that utilizes statistical analysis to minimize defects and improve process efficiency.
- Culture: A supportive organizational culture enhances BPM values and fosters an environment conducive to BPM success, although culture-related efforts may have a longer time horizon for significant impact compared to other factors.

FUTURE TECHNOLOGY

Heathrow Airport and the Rise of Digital Air Traffic Control Towers

England's Heathrow Airport, one of the busiest airports globally, exemplifies the challenges faced by traditional air traffic control (ATC) methods. Managing the complex flow of aircraft relies on human controllers stationed in a physical tower, with limitations in visibility and potential inefficiencies. For decades, ATC has relied on a well-established system: Controllers stationed in physical towers utilize radar and visual observation from windows to manage aircraft movements. While effective, this method has limitations, such as sight being compromised by low visibility conditions like fog or cloud cover, existing towers becoming geographically unsuitable as airports expand, the slowness and potential imprecision of manual methods for estimating aircraft turnaround times, and a shortage of qualified air traffic controllers.

Digital ATC towers present a potential paradigm shift in air traffic management. These systems leverage cutting-edge technologies, such as high-definition cameras that create a panoramic view of runways and surrounding areas, AI-powered image analysis that can identify objects like support vehicles and overlay radar data on each aircraft for easier identification, and machine learning that automates tasks like turnaround time estimation and runway clearance in low visibility conditions, freeing up controllers for critical decision-making.

17 Jan vom Brocke and Michael Rosemann, eds., *Handbook on Business Process Management 1: Introduction, Methods, and Information Systems* (Springer, 2015).

Heathrow has actively explored the potential of digital ATC towers. In collaboration with NATS, the UK's ATC provider, they have implemented a trial system at the airport. This system utilizes high-definition cameras and AI algorithms, demonstrating the potential benefits of enhanced visibility, improved efficiency, and remote operation.[18]

Despite the promising advancements of digital ATC towers, there are challenges to consider. Regulatory bodies like the Federal Aviation Administration in the United States have yet to fully certify digital towers, hindering widespread adoption. Transitioning to digital towers may require retraining or relocating existing air traffic controllers, potentially impacting jobs. And while AI can be a valuable tool, complete dependence on automation could pose safety risks. Human expertise remains crucial. The digital ATC tower revolution is in its early stages, but it represents a significant potential disruption to the traditional air traffic control landscape.

Information Systems and Business Processes

By capturing and managing data, monitoring performance, and facilitating communication, information systems contribute to improved efficiency, better decision-making, and overall business growth for any business process. Following are the primary areas in which information systems play a vital role:

- Capturing and storing process data: Capturing and storing relevant data generated during business processes is one of the fundamental tasks of an information system. These data can come from various sources such as transactions, customer interactions, and inventory updates. For example, a retail store's information system records each sales transaction, including the products sold, quantity, and customer information. These data are then stored in a database for further analysis, reporting, and decision-making.
- Monitoring process performance: Information systems are also responsible for monitoring the performance of business processes. This involves tracking key performance indicators and metrics to assess how well a process is functioning and whether it meets the desired objectives. For instance, an e-commerce platform's information system might track website traffic, conversion rates, and customer satisfaction to evaluate the effectiveness of its online sales process. In some cases, these monitoring tasks are fully automated. For instance, an information system can generate real-time reports and alerts when certain performance thresholds are reached or breached. This automation ensures that the organization can respond promptly to issues and make informed decisions.
- Facilitating communication and coordination: Another important role of information systems is to facilitate communication and coordination among different functional areas within the organization. As businesses grow, the complexity of operations increases, and different departments need to work together seamlessly. Information systems enable smooth information flow, allowing employees from various departments to collaborate effectively. For example, a company's enterprise resource planning (ERP) system integrates information from different departments, like finance, human resources, and supply chain, ensuring a coherent flow of data and streamlined processes.

It is important to be aware that the level of automation in these roles can vary. Some tasks are fully automated, meaning the information system handles them entirely without human intervention. In contrast, other tasks require human input, where the information system relies on the judgment, expertise, and intuition of managers to make decisions based on the information provided.

LINK TO LEARNING

Learn about developments in CRM technology (https://openstax.org/r/109ITusingAI) and how AI can

18 "London's Heathrow Airport Trials AI to Revolutionise Air Traffic Control," *London Daily News*, December 3, 2024, https://www.londondaily.news/londons-heathrow-airport-trials-ai-to-revolutionise-air-traffic-control/

generate value in business for customers using IT.

2.5 Digital Innovation Creation, Distribution, and Commercialization

Learning Objectives

By the end of this section, you will be able to:

- Discuss digital innovation, and steps to create a digital innovation
- Identify ways to integrate information technologies to innovate and transform an organization's offerings

Digital innovation continues to change the way we live. For example, Rio was a brand of portable digital audio players, first introduced in 1998 by the Diamond Multimedia company. iTunes was a media player, media library, and online store developed by Apple Inc. first released in 2001. In 2003, Apple introduced the iTunes Store, where users could purchase and download digital music, movies, and TV shows. The key difference between Rio and iTunes is that Rio was a dedicated hardware device (portable MP3 player), whereas iTunes started as software that could be used on computers. This made downloading music easy and convenient. Over time, Apple integrated iTunes with their iPod line of portable devices, creating a seamless ecosystem for purchasing, managing, and syncing digital content between computers and iPods. Rio was unable to compete with this new model, and the company discontinued them in 2005. Apple's true innovation was the digital innovation of making the downloading of music easy and convenient by leveraging technology. More and more, organizations face mounting pressure to adopt digital technologies to revitalize and revolutionize their business models and adapt to ever-evolving digital trends.

In 2020, the rapper Travis Scott teamed up with the popular online video game Fortnite for a virtual concert titled "Astronomical." This event was remarkable for its integration of virtual technology within the gaming platform, attracting over twenty-seven million unique players who participated live across five days. It set a significant benchmark for the future of virtual music festivals, showcasing the potential for immersive digital experiences.[19] Similarly, in response to the pandemic in 2020, the iconic event Burning Man transitioned to a virtual "Multiverse" leveraging VR technology to re-create its distinct atmosphere. Through dynamic 3D art installations, themed camps, and musical performances staged in various virtual locations, participants could still immerse themselves in Burning Man's ethos, highlighting the resilience of community spirit and cultural exchange in a digital age. These examples illustrate how technology continues to revolutionize the way we experience music concerts and festivals, offering immersive alternatives that transcend geographical limitations and redefine traditional event formats. These VR concerts enable fans to experience performances from anywhere in the world, breaking geographical barriers.

Digital Innovation and Its Adoption

In management information systems (MIS) scholars have identified two main perspectives on innovation and its relation to IS. These perspectives offer valuable insights into how organizations adopt and leverage digital technologies to drive progress. The first perspective, known as "IT innovation," focuses on how organizations integrate new IT-enabled business processes, products, and services. Simply put, this type of innovation refers to the adoption of an already-existing IT product or service that is new to an organization.

The second perspective, **digital innovation**, centers on a product-oriented approach that examines how the combination of physical and digital products leads to the creation of entirely new offerings (Figure 2.9).[20] This perspective also delves into the role of IT in facilitating or constraining the development of innovative products. By studying digital innovation, we gain insights into how organizations structure and manage their innovative endeavors more effectively.

19 Dave Thier, "A Staggering Number of People Saw Fortnite's Travis Scott 'Astronomical' Event," *Forbes*, April 28, 2020, https://www.forbes.com/sites/davidthier/2020/04/28/a-staggering-number-of-people-saw-fortnites-travis-scott-astronomical-event/

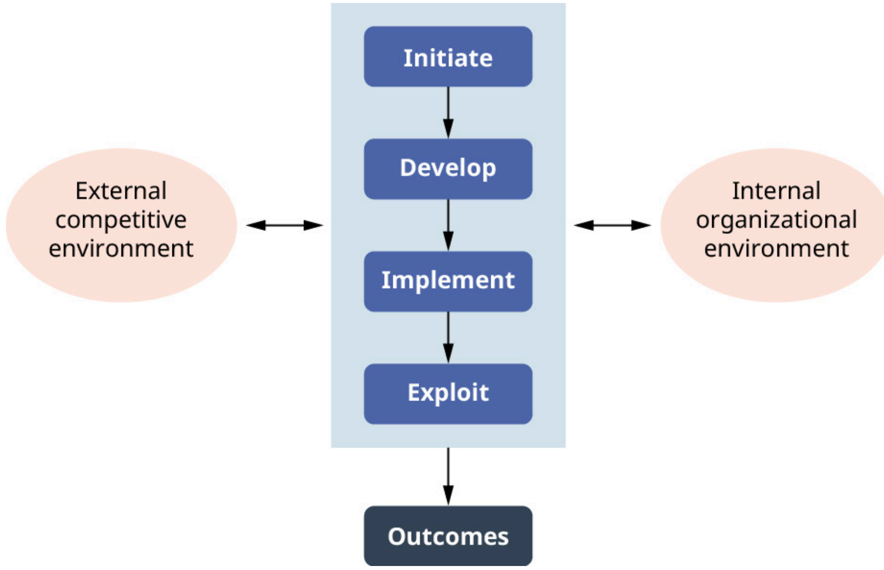


Figure 2.9 The process of digital innovation follows distinct steps and is informed by the external competitive environment and the internal organizational environment to produce the desired outcomes. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Digital innovation encompasses a range of activities that include initiation, development, implementation, and exploitation. The first, initiation, involves the process of identifying and acquiring information on business processes and requirements from both internal and external sources within the organization. The goal is to find problems and opportunities that are well-suited for digital innovation—areas where implementing digital solutions can lead to significant improvements or create new opportunities for growth. For instance, there may be increasing demand for renewable energy sources and a need to reduce greenhouse gas emissions. This realization may prompt a company to explore opportunities in the renewable energy sector and invest in new digital technologies to address these challenges.

Development focuses on the creation and design of new information systems. It encompasses various activities such as building entirely new solutions from scratch, customizing existing systems to better fit an organization's needs, or adopting preexisting solutions that have proven to be effective elsewhere. The development phase lays the foundation for digital innovation to be implemented successfully. For instance, a company might invest in research and development to create advanced digital monitoring systems for its offshore oil platforms. These systems should leverage cutting-edge technology to minimize environmental impact.

Once the digital innovation has been developed, the implementation phase begins. This involves the actual installation and deployment of the information system within the organization. Beyond the technical aspect of installation, it also includes ensuring that the new systems are integrated into the organization's existing structure and processes. This may require setting up new governance systems, providing appropriate training to employees, and establishing new processes to support digital innovation. This may also involve installing digital systems in an organization's satellite locations and providing the training its workforce needs to use the technologies effectively. The organization may also offer incentives to encourage employees to adopt and embrace the new digital tools.

Exploitation refers to maximizing the value derived from the existing information system. After implementation, organizations leverage these systems to their fullest potential. This may involve reusing existing systems and technologies for different purposes, finding innovative ways to utilize the data collected by these systems, and continuously extracting value from the digital innovations to drive growth and efficiency. For instance, after digital innovation has been implemented, a company's new advanced monitoring

20 Rajiv Kohli and Nigel P. Melville, "Digital Innovation: A Review and Synthesis," *Information Systems Journal* 29, no. 1 (2018): 200–223, https://doi.org/10.1111/isj.12193.

systems may not only improve safety and efficiency but now also provide new data insights. The company could leverage this data to optimize its operations further, forecast maintenance needs, and enhance overall performance.

Other important aspects of digital innovation are the internal organizational environment, the external competitive environment, and the outcomes. The internal organizational environment refers to the organizational backdrop in which digital innovation takes place. It includes factors such as the organization's business and data strategies, how data are managed and shared within the organization, and the established business processes for doing things. The internal organizational environment heavily influences how effectively digital innovation will be adopted and integrated into the organization. The external competitive environment encompasses the broader market in which the organization operates. It includes factors such as industry trends, market fads, the behavior of competitors, and the preferences of consumers. Understanding the external competitive environment is crucial for organizations to ensure their digital innovations align with market demands and offer a competitive advantage. The outcomes of digital innovation refer to the end results achieved by adopting and implementing digital solutions. These outcomes can be either projected or actual results. Projected outcomes are the anticipated benefits and improvements expected from the digital innovation, while actual outcomes represent the tangible results realized after the implementation. These outcomes often include new and improved business processes, innovative products, and more efficient services that contribute to the organization's overall success.

It is essential to note that not all of these components are mandatory in every digital innovation effort, and they need not follow a prescribed order. In practice, these activities may intertwine to such an extent that it would be challenging to distinguish them.

Deploying Information Technologies to Innovate

Given that not every company starts with digital products and services, nor can every company benefit from them, the question arises: How should an organization pursue digital innovation or consider transforming its products in the digital age? The simple answer is that developing an understanding of the unique context of a business and adopting a well-defined framework can help the organization successfully leverage digital technologies to enhance its products and services, foster growth, and remain competitive in the digital age. A comprehensive framework that sheds light on how products and services can harness digital innovation consists of three popular approaches: opening the door to third parties, connecting customers, and connecting products in order to connect customers.[21]

Opening the door to third parties refers to creating an ecosystem that allows external developers and businesses to integrate their products or services into the primary platform, thereby expanding its functionality and value for end users. This approach can transform a traditional product into a robust platform that caters to a broader range of needs and attracts a larger user base. Gojek is an Indonesian technology company that initially started as a ride-hailing and courier service. Over time, the company recognized the opportunity to expand its platform beyond transportation and ventured into various other services, including food delivery, grocery delivery, parcel delivery, digital payments, and more. To achieve this expansion and provide diverse services to its users, Gojek adopted the "opening the door to third parties" strategy. It created an open platform that welcomes third-party service providers to offer their services through the Gojek app. For instance, local restaurants can partner with Gojek to offer food delivery services, and independent drivers can register to provide ride-hailing services through the Gojek platform.[22] By integrating numerous third-party services into its app, Gojek has become an all-in-one super app, catering to a wide range of everyday needs for millions of users.

Connecting customers involves creating a platform that facilitates interactions and transactions between

21 Andrei Hagiu and Elizabeth J. Altman, "Finding the Platform in Your Product," *Harvard Business Review* 95, no. 4 (July–August 2017): 94–100.

22 Marc Steinberg, Rahul Mukherjee, and Aswin Punathambekar, "Media Power in Digital Asia: Super Apps and Megacorps," *Media, Culture & Society* 44, no. 8 (2022): 1405–1419. https://doi.org/10.1177/01634437221127805

customers, essentially forming a marketplace where buyers and sellers can connect with each other directly. This approach transforms the product into a platform that not only serves customers directly but also enables them to engage with each other, leading to increased network value for all participants. Instagram, a popular social media platform owned by Meta, started out primarily as a photo-sharing app where users could post pictures and videos to share with their followers. As the platform grew in popularity, businesses and individual sellers recognized its potential as a marketing and e-commerce tool. To capitalize on this opportunity, Instagram introduced Instagram Shopping, which allows businesses and individual sellers to set up virtual shops directly on the platform, showcasing their products through photos and videos. Users can explore these shops, browse products, and make purchases without leaving the app. By enabling this direct connection between sellers and potential buyers, Instagram became more than just a social media platform—it became a thriving marketplace where businesses could reach a large audience and customers could discover and purchase products seamlessly.

Connecting products to connect customers involves creating a platform that connects various products or services to offer a comprehensive and seamless experience to customers. This approach aims to provide customers with a unified ecosystem where different products work together harmoniously, creating convenience and value for users. By connecting products, companies can strengthen customer loyalty, increase engagement, and establish a dominant position in their respective markets. Microsoft's Windows operating system exemplifies the strategy of connecting products to connect customers. Windows is a platform that serves as the foundation for running a wide variety of software applications on personal computers. Microsoft recognized that by creating a unified ecosystem and connecting different software products to the Windows platform, it could increase its value and attract a larger user base. As a result, a vast array of applications, ranging from productivity tools to creative software and games, were made available to Windows users. This interconnected ecosystem made Windows an indispensable platform for PC users, as they could seamlessly install and use various software products for their specific needs. The availability of a diverse selection of software products contributed to the success and widespread adoption of the Windows operating system.

Key Terms

advertising model digital business model that generates revenue through targeted ads purchased by other businesses

affiliate model digital business model in which one company earns commissions by promoting and selling other companies' products or services through websites or social media channels

analytic data type of structured datathat include aggregated and summarized data from various sources and enables in-depth analysis, reporting, and decision support

big data large datasets that are complex in volume, variety, veracity, and volume and that require specialized processing techniques to extract valuable insights and make informed decisions

business process continuous series of interconnected activities aimed at producing a valuable product or service for an organization, its business partners, and its customers

business process improvement (BPI) evaluation of existing business processes to identify areas for improvement

business process management (BPM) ongoing review and analysis of processes across an organization to identify opportunities for improvements or reengineering that will optimize core business processes

business process reengineering (BPR) radical rebuilding of core business processes to achieve optimization

competitive advantage conditions and circumstances that enable a company to compete more effectively than its rivals in a given market

crowdfunding model digital business model that raises funds for a product, project, or idea through an online platform, leveraging the collective support of the public

data definition instruction for how to organize information

data governance policies, procedures, and standards that determine how an organization manages the availability, usability, integrity, and security of an organization's data throughout the data life cycle

data integrity accuracy and consistency of data throughout their entire life cycle

decision-making framework breaks down decisions into two types: programmed decisions with clear procedures or nonprogrammed decisions requiring more judgment

design thinking approach to problem solving that uses creativity and empathy to understand user needs in order to create user-centric products and services

digital innovation perspective of management information systems that examines how the combination of physical and digital products leads to the creation of entirely new offerings

digital product model digital business model offering downloadable digital assets that may include actual products, such as e-books, or may be used to provide information such as assembly instructions or details about a product's components

e-commerce model digital business model that involves buying and selling goods or services online through websites or apps, and offers convenient shopping experience for various customer segments

freemium model digital business model offering a free basic service, with the option to upgrade to a premium version for enhanced features or benefits

functional area information system (FAIS) information system designed to support specific business functions within an organization

information quality accuracy, completeness, consistency, and timeliness of data

marketplace model digital business model that brings buyers and sellers together on a single platform, with the enterprise acting as an intermediary that facilitates transactions between parties

master data type of structured data that represent core entities such as customers, products, or employees

operational data type of structured data that include transactional data generated by day-to-day business operations

reference data type of structured data that include codes, classifications, or standards used across the organization

Robert Anthony framework divides a problem, and by extension the data needed to resolve this problem, into three domains: operational control, management control, and strategic planning

sharing economy model digital business model in which individuals share resources or services through a peer-to-peer network, enabling efficient utilization of underused assets

strategic planning process of defining an organization's mission, vision, goals, and objectives, and developing strategies to achieve them, often with the support of information systems, typically done by senior level managers

subscription model digital business model offering continuous value through recurring subscriptions that provide customers with ongoing premium content or services

variety key dimension of big datathat encompasses the diverse array of data types and formats

velocity key dimension of big data that describes the rapid pace at which data are generated and collected, thereby necessitating real-time processing

veracity key dimension of big data that refers to the reliability, accuracy, and trustworthiness of the data, considering factors like data quality and consistency

volume key dimension of big data that refers to the vast amount of data generated and stored

Summary

2.1 Practices and Frameworks for Data Management

- Data governance involves establishing policies, processes, standards, roles, and responsibilities to manage data as a valuable asset. One important part of data governance is information quality, which covers how accurate, complete, consistent, and readily accessible it is.
- Data management is about figuring out the specific ways that data will be stored, analyzed, protected, and measured.
- Data quality involves ensuring that data are accurate, complete, and consistent.
- The four key dimensions of big data—known as the four *V*s—include volume, variety, velocity, and veracity.
- Different types of data are required for generating suitable information, and different types of data require different management approaches. There are two main categories of data: structured data and unstructured data.
- Good data management strategies require updating outdated data, rectifying known inaccuracies, addressing varied definitions, resolving discrepancies in redundant data sources, and managing variations in opinions, forecasting techniques, or simulation models.
- Information systems planning and management involve selecting and implementing the right technology infrastructure for data storage, processing, analysis, and governance.
- There is a distinction between information used for strategic planning and information used for management control. Strategic planning focuses on the long-term goals and direction of the company, while management control ensures efficient day-to-day operations and adherence to those strategic plans.
- Foundational frameworks include the Robert Anthony framework, Herbert A. Simon’s decision-making framework, and Gorry and Scott Morton’s framework, which combines elements of both the Robert Anthony framework and Simon’s decision-making frameworks.

2.2 Strategies to Improve the Value of Information Technology Within Organizations

- Information technology systems are used in handling tasks that involve high degrees of uncertainty and take place in dynamic and unstructured situations.
- The most common means of understanding the value of IS in a business is to measure the relationship between IT investments and output measures of revenue and human productivity. However, the business value of IT goes beyond direct output or revenue measures because IT often supports organizational redesign efforts.
- Data managers decide whether they need IT systems for operational purposes or for strategic planning.

- Managers see that IT can bring value through three primary methods, including automation of operation, information generation for managing people and resources, and transformation of existing processes or combined tasks.
- Functional area information systems (FAIS) are designed to enhance the internal efficiency and effectiveness of each department in an organization by providing valuable support tailored to each respective department's functions.
- Business-IT alignment, or strategic alignment, refers to the strong integration of the IT function with an organization's strategy, mission, and objectives.
- Gaps between business and IT departments can usually be attributed to different objectives, lack of expertise awareness, and lack of communication.
- To improve business-IT alignment, organizations should prioritize organizational communication, focus on strengthening their governance, align scope and IT architecture, and emphasize the development of human skills.
- The five key strategies usually pursued by organizations when seeking to generate value include IT cost leadership strategy, differentiation strategy, focus/innovation strategy, operational effectiveness strategy, and customer-oriented strategy.

2.3 Digital Business Models

- Organizations need to develop digital business models that deliver value to customers or users by working as the vital connector between technology and the strategic goals of an organization.
- A successful business model provides a logical framework that unlocks the hidden value of technologies, allowing businesses to benefit economically, as well as serving as a blueprint for how a company generates and captures value from new products, services, or innovations.
- Common digital business models include e-commerce, subscription, freemium, affiliate, marketplace, advertising, crowdfunding, sharing economy, and digital product.
- Digital business models face criticisms and challenges including unequal distribution of opportunities, level of control in algorithmic systems, and lack of transparency.

2.4 Business Process Management

- The business process relies on three essential components: inputs, resources, and outputs.
- Efficient and well-designed business processes are crucial for gaining a competitive advantage and ensuring organizational success. Functional areas in the business process include accounting, finance, marketing, production/operations, human resources, and management.
- Measures of excellence when evaluating the execution of a business process include user satisfaction, innovation, flexibility and adaptability, cost reduction, quality, differentiation, customer satisfaction, environmental impact, and compliance and governance.
- Key parameters in BPM that contribute to the successful digitalization of business process initiatives within an organization include strategic alignment, methods, and culture.
- By capturing and managing data, monitoring performance, and facilitating communication, information systems contribute to improved efficiency, better decision-making, and overall business growth for any business process.

2.5 Digital Innovation Creation, Distribution, and Commercialization

- In management information systems, IT innovation focuses on the integration of new IT-enabled business processes, products, and services within an organization, while digital innovation centers on the creation of new offerings through the combination of physical and digital products and examines IT's role in facilitating or constraining innovation.
- The steps involved in digital innovation are initiation, development, implementation, and exploitation, which are informed by the external competitive environment and the internal organizational environment. Not all of these components are mandatory in every digital innovation effort, and they need not follow a

prescribed order.

- Digital platform strategies include opening the door to third parties, which creates an ecosystem for external developers to integrate their products/services, enhancing platform functionality; connecting customers, which facilitates interactions and transactions between customers, forming a marketplace; and connecting products to connect customers, which links various products/services to provide a comprehensive, seamless customer experience.

Review Questions

1. Which parameter of data management focuses on safeguarding personal data from unauthorized access, use, disclosure, disruption, modification, or destruction?
   a. data security
   b. data governance
   c. data privacy
   d. data architecture
2. Which dimension of big data characterizes the rapid pace at which data is generated and collected, which necessitates real-time processing?
   a. variety
   b. velocity
   c. veracity
   d. volume
3. In the Robert Anthony framework, which domain ensures that an organization is meeting its strategic goals through activities such as setting budgets and tracking sales?
   a. strategic planning
   b. operational control
   c. intelligence
   d. management control
4. Which functional area's overall value indicators for information technology investment include improved product quality and streamlined processes?
   a. supply chain management
   b. manufacturing and operations
   c. research and development
   d. information technology and technology management
5. Collaboration is one of the six key characteristics needed for successful business-IT alignment. What does collaboration mean?
   a. Clear overarching goals are established and understood by both information technology and business employees.
   b. The organization fosters a vibrant and inclusive company culture.
   c. Business and information technology professionals are cross-trained and move across different departments and job roles.
   d. Information technology is considered a driver of innovation that continuously transforms the business, leading to new revenue opportunities.
6. Which strategy to generate value using information systems seeks to distinguish a business's products and/or services from those of competitors?
   a. differentiation strategy
   b. operational effectiveness strategy
   c. focus/innovation strategy
   d. cost leadership strategy

7. Which business model earns commissions by promoting and selling other companies' products or services through websites or social media channels?
   a. affiliate model
   b. e-commerce model
   c. marketplace model
   d. sharing economy model
8. What has caused opacity and a lack of transparency in online platform–based work?
   a. standardized metrics and homogenized worker identities
   b. unequal distribution of opportunities
   c. algorithmic control systems
   d. proprietary algorithms protected by trade secrecy laws
9. Which component of the business process is the backbone of process activities, ensuring that tasks in the process are completed?
   a. inputs
   b. resources
   c. outputs
   d. interconnected activities
10. What tool enables information systems to promote business success by monitoring process performance?
   a. inventory updates
   b. key performance indicators
   c. A/B testing
   d. process modeling
11. Which digital innovation activity refers to maximizing the value derived from the existing information systems?
   a. initiate
   b. develop
   c. implement
   d. exploit
12. Which approach to digital innovation forms a marketplace where buyers and sellers can interact with each other directly?
   a. opening the door to third parties
   b. connecting customers
   c. connecting products to connect customers
   d. leveraging digital technologies

Check Your Understanding Questions

1. Define data governance.
2. What are unstructured data? Include examples and explain the value of unstructured data that makes them worthwhile to manage despite challenges.
3. In Simon's decision-making framework, what three-step process is used to determine which activities are programmable and which ones are nonprogrammable? Explain each step.
4. How does an organization view information technology as a strategic partner driving innovation and new revenue opportunities?
5. How does an organization prioritize the needs of internal and external customers, with a focus on excellent customer service?

6. How can you determine whether there is a culture of cross-training and collaboration between business and information technology professionals?
7. How are clear overarching goals established and understood by both information technology and business personnel?
8. How does the freemium business model differ from the subscription business model?
9. How can digital business models lead to unequal opportunities for platform workers?
10. How can algorithmic control in digital platforms be problematic?
11. How can an organization assess whether the business processes of an information system are well designed?
12. How can analyzing the business processes of an information system help an organization identify potential areas for improvement and gain a competitive advantage?
13. How can information technology serve as a pivotal catalyst in facilitating transformative change through business process reengineering?
14. What are the two main perspectives in management information systems regarding innovation and its relationship with information systems? Briefly describe each one.
15. What key activities are involved in digital innovation, and how do they contribute to organizational success?
16. How does the "opening the door to third parties" approach contribute to digital innovation, as exemplified by Gojek?
17. What is the significance of the "connecting customers" approach in digital innovation, as illustrated by Instagram?
18. How does the "connecting products to connect customers" approach contribute to digital innovation, as demonstrated by Microsoft's Windows operating system?

Application Questions

1. On December 23, 2021, the accounts of more than three million users of the U.S.-based FlexBooker appointment scheduling service were stolen and being traded on hacker forums. Customers were businesses needing to schedule appointments. This ranged from professionals like accountants and lawyers to service providers like hairdressers and dentists to owners of facilities like gyms and repair shops. Do some research on whether FlexBooker was following the best data security practices? Did it have well-defined user roles for who could access its data?
2. In January 2020, Microsoft acknowledged that a customer support database containing anonymized user analytics had been accidentally exposed online. The data breach involved email addresses, IP addresses, and other details stored in the company's customer support case analytics database. The exposed database contained over 250 million Microsoft customer records spanning fourteen years, without any password protection. Microsoft attributed the server exposure to misconfigured Azure (a cloud platform with data-related services) security rules implemented on December 5, 2019. Upon discovering the issue, Microsoft quickly addressed the configuration problem to prevent unauthorized access. How do you think this incident impacted clients of Azure, and what could they have done differently? Do some additional research to back up your answer.
3. Imagine you are working on information technology strategy for a small local café in competition with a large fast-food chain like McDonald's. If the small café wants to introduce a fancy new mobile app for customization of orders to improve customer experience, how would you evaluate the value and feasibility

of this information technology investment?

4. Imagine you are an information system consultant, and you have been given a report from an organization’s business analysts that indicates that investments in information systems are projected not to affect the company’s efficiency or productivity and not to impact its revenue. Would you recommend that the organization proceed with such investments? Why or why not?
5. Access the Clean Eatz (https://openstax.org/r/109CleanEatz) website. Prepare a list of all the services the company provides. Identify its digital business model and describe the information technology strategy implemented.
6. Access the The Knot (https://openstax.org/r/109TheKnot) website. Identify its digital business model and describe the information technology strategy implemented.
7. Enter the Alibaba.com (https://openstax.org/r/109Alibaba) website. Identify its digital business model and describe the information technology strategy implemented. How can such a site help a person who is making a purchase?
8. Your IS team is debating which of two images for your website’s home page are more likely to appeal to website visitors. What process do you recommend to help the team make this decision and why?

3

Database Management Systems

Figure 3.1 Databases are regularly used in businesses to organize large amounts of data and require an understanding of database management systems. (credit: modification of work "DARPA Big Data" by Defense Advanced Research Projects Agency (DARPA)/Wikimedia Commons, Public Domain)

Chapter Outline

Introduction

Databases play a significant role in everyday life, even if they are unnoticed. From organizing personal photos and contacts on a phone to keeping track of inventory at a grocery store, databases help manage and make sense of the vast amounts of information we encounter every day. IS professionals should understand the fundamentals of database management systems, how they are used to address business problems, and how they are applied practically. Whether it is a mobile app or a cloud-based system, databases are key to the tools and systems that businesses rely on, making it essential to understand how they work and how to design them effectively.

3.1 Data Types, Database Management Systems, and Tools for Managing Data

Learning Objectives

By the end of this section, you will be able to:

- Define data and differentiate between types of data
- Identify tools and techniques for managing data with database systems
- Determine how to gather, organize, curate, and process data
- Compare and contrast database management systems

Understanding the fundamentals of data is important for effective management. Data can be categorized into structured, semistructured, and unstructured forms, requiring different tools and techniques to collect and analyze. Effective data management involves collecting, storing, and processing data using tools like a database management system (DBMS).

Identifying the business problem of an organization involves understanding the organization's goals and opportunities through comprehensive needs analysis and stakeholder engagement, which involve collecting and analyzing data. By leveraging well-managed data, organizations can gather accurate user requirements to ensure their solutions align with the end users' needs and expectations. These solutions are often built on robust database design and management practices, which are essential for creating scalable and efficient data systems. Careful planning, structuring, and management of data ensure databases support current and future needs. Effective database management includes regular tasks such as backup and recovery of data, performance optimization, and security enforcement. Additionally, as organizations continue to develop their data capabilities, the need for reliable mobile database development has become more prominent.

A mobile database is a database used on mobile devices, such as a smartphone or tablet, to store and access data. It must be lightweight to save storage, use less power, and work efficiently on limited mobile device resources. A cloud-based database is a database system stored and managed online. It allows the user to access it through the internet instead of keeping it on a single device. The development and integration of these database types has revolutionized how organizations store, manage, and analyze data, offering scalability, flexibility, and cost-effectiveness. Integrating mobile and cloud databases connects mobile devices with centralized storage, making it easy to sync, access, and manage data across platforms. This creates a smoother and more efficient way to handle data for businesses.

Types of Data

Understanding how to manage data is important for any organization in the digital world. Data, as you learned in 1.1 Introduction to Information Systems, consist of any information that can be processed or analyzed to gain insights and make decisions. Data come in two main categories line of business data and customer behavior data. Line of business data consists of the information generated from daily business operations, such as financial records, day-to-day operations, inventory processes, and supply chain details. These data are important for running the business efficiently. Customer behavior data consists of information collected about how customers interact with the company's products or services. This includes a customer's frequent transactions, purchase history, browsing patterns, social media interactions, and feedback.

These types of data can appear in various forms, such as text, voice, and images. Text data include emails, documents, news, and social media posts. Voice data come from customer service calls or voice-activated devices. Image data include photos and scanned documents, while video data consist of recordings from security cameras, social media, or marketing videos. There are three types of data: structured, semistructured, and unstructured (Table 3.1). Data that are highly organized and easily searchable is called **structured data**. Structured data is found in spreadsheets, tables, or databases. Another type of data is **semistructured data**, which are data that have some organization but does not fit neatly into tables. Two examples of semistructured data are extensible markup language (XML), which is a way to organize data using tags so that both people and computers can read it, and JavaScript Object Notation (JSON) files, which are in a format that transmits and stores data using human-readable text. This format can be used to send information from a web application to a database to migrate data. Finally, **unstructured data** lack a predefined structure and require advanced techniques for analysis; these include emails, videos, and social media posts.

	Structured Data	Semistructured Data	Unstructured Data
Definition	Highly organized and formatted data, easily searchable in databases	Partially organized data with some structure; tags often used to separate data elements	Data lack any specific structure, making it difficult to search and analyze directly
Examples	SQL databases, spreadsheets	XML, JSON, email	Text documents, images, videos, social media posts
Storage	Stored in tables with rows and columns	Stored in formats that contain tags	Stored as binary or text files, often in large volumes
Ease of access	Easy to query	Moderately complex	Highly complex
Scalability	Moderate, depends on the database system	High, designed to handle large volumes of data	High, but requires significant resources
Usage	Financial records, inventory systems	Web data, configuration files	Multimedia content, big data analytics, social media
Tools	Relational database management systems	NoSQL databases, XML, JSON parsers	Big data platforms (Apache Hadoop, Spark)
Performance	High for structured queries	Moderate, depends on the complexity of the structure	Variable, depends on the tools and methods used for analysis

Table 3.1 Comparison of Structured, Semistructured, and Unstructured Data Understanding the different types and forms of data is crucial to effectively manage and use the information to drive business decisions and strategies.

In 2006, British mathematician and data scientist Clive Humby compared data in the digital age to oil in the past, highlighting the crucial role of data in organizational growth.[1] Just as oil powered the industrial age, data fuels the integration of digital technology into nearly all business, production, and industry processes; this integration is known as Industry 4.0. Effective use of data is vital to the successful operation of modern organizations. Data help in understanding market trends, customer behaviors, and organizations' internal processes, which is essential for making informed decisions, improving efficiency, enhancing customer experiences, and fostering innovation.

Managing Data in a Database Management System

A **database management system (DBMS)**, which is a software system that manages, stores, and processes data, ensuring the data are organized, accessible, and secure. For example, a large hospital network uses a DBMS to streamline patient care and administrative tasks and support operations such as the following:

- Electronic health records (EHRs): Patient medical histories, prescriptions, lab results, and imaging files are stored in a centralized database, allowing doctors to access up-to-date information instantly.
- Appointment scheduling: Doctor availability and patient schedules are tracked to avoid conflicts and

1 Clive Humby, "Data Is the New Oil," (lecture at Association of National Advertisers conference, Orlando, FL, April 30–May 2, 2006).

reduce wait times.
- Billing and insurance processing: A DBMS automates billing, tracks payments, and verifies insurance claims efficiently.
- Real-time alerts: A DBMS sends reminders for follow-up visits or medication refills and flags potential drug interactions or critical lab results for immediate review.

When you request a ride from a company like Uber or Lyft, or make a purchase at a grocery store, a DBMS is working in the background to handle all the information needed to make things run smoothly. A ride-sharing app collects information like the following:

- your current location and where you want to go
- available drivers nearby
- traffic conditions to calculate the best route and estimated time
- payment details to process the fare

After the ride, the data doesn't just sit there. It's used to

- figure out where and when ride requests are most common,
- help drivers be in the right place at the right time, and
- improve routing and reduce delays.

By organizing and analyzing data effectively, a DBMS helps businesses make better decisions, save money, and improve customer experiences.

These systems organize and store large amounts of data efficiently, allow easy access and querying of data, ensure data accuracy, control data access, handle data transactions, guarantee data reliability, support large-scale data operations, ensure high performance, and provide mechanisms to restore data in case of failures.

Managing data effectively is essential for organizations, and database systems provide a structured environment to store, retrieve, and manipulate data efficiently. Various tools and techniques are used to manage data within these systems, each catering to different types of data and requirements. At the core of effective data management are two fundamental issues: how to use a database and how to build a database. Addressing these issues involves a variety of tools and techniques that are designed to ensure a high quality of data management.

The tools and techniques for using a database include the following:

- Structured Query Language: **Structured Query Language (SQL)** is the standard language used to query and manage data in relational databases. It allows users to perform a wide range of operations such as SELECT, INSERT, UPDATE, DELETE, and JOIN to handle data efficiently. For example, in a ride-sharing app like Uber or Lyft, when a user requests a ride, the app's database must quickly identify nearby drivers.
- Database management systems: As mentioned previously, DBMSs manage data storage, and software like MySQL, PostgreSQL, Oracle Database, and Microsoft SQL Server provide the interface and tools necessary for database interaction.
- Database access tools: A **database access tool**, such as SQL Server Management Studio, provides graphical user interfaces (GUIs) to facilitate database interaction without writing extensive code.
- Indexing: Creating indexes on database tables improves the speed of data retrieval operations. Indexes are especially useful for large databases where query performance is critical. For example, in social media platforms like Instagram or X, millions of posts are created every second. When a user opens the app, the database must quickly retrieve the most recent posts from accounts they follow. An index on the user_id column ensures quick filtering of posts by the accounts that users follow. Another index on the created_at column allows the database to instantly sort posts by the most recent time stamps. This allows the app to load the user's feed almost instantly, even with billions of posts in the database, providing a seamless user experience.

- Transactions: Data consistency and integrity are protected by adhering to **ACID (atomicity, consistency, isolation, and durability)** properties. These ACID characteristics ensure that a transaction is all-or-nothing (atomicity), keeps the database accurate and adhering to rules (consistency), prevents transactions from interfering with each other (isolation), and guarantees that once a transaction is complete, it stays saved even if the system crashes (durability).
- Backup and recovery: Regular backups and effective recovery plans are vital for data protection. Tools like mysqldump, pg_dump, and RMAN (Oracle Recovery Manager) help in creating backups and restoring data when necessary.
- User access management: Managing user permissions and roles ensures that only authorized users can access or manipulate the data. The DBMSs provide tools to define user roles and privileges.

Building a database involves two steps—design and implementation—to ensure that a structure can efficiently store and manage data. The database design involves creating an entity relationship diagram (ERD), which is a visual representation of the database structure, including entities, attributes, and relationships. Entities are the things we are keeping data about, like “students,” or “classes.” Attributes are the details about an entity, like a student’s name or date of birth. Relationships show how entities are connected, like a student being enrolled in a class.

A technique used in the design process is normalization, in which data are organized and stored only once to eliminate the duplication of data. This helps to ensure data consistency and integrity and reduce redundancy. Tools like Lucidchart can help facilitate the design process. This involves dividing large tables into smaller, related tables and defining their relationships. Another important step in the design process is defining the **database schema**, which is the structures of tables, including columns and data types. This step is followed by using a data modeling tool like Microsoft Visio, which assists in creating and visualizing the database schema, helping to design both the logical and physical aspects of the database. Finally, it is important to implement data security measures such as encryption to protect sensitive data. A DBMS provides features and tools to enforce data security policies, ensuring that data remain safe and compliant with regulations. Data security policies in a DBMS can come from both the organization and federal regulations. Organizational policies are rules set by the company, like allowing only human resources to access salary records. Federal policies are legal requirements, like the Health Insurance Portability and Accountability Act (HIPAA), which protects patient health information.

Database Types

Data storage is fundamental to how information is organized and accessed in computing environments. Here are some key types of databases:

- A **relational database** stores data in tables with rows and columns, making it ideal for structured data. Each table contains data about a specific type of entity, and tables can be linked using keys (MySQL).
- A **NoSQL database (Not Only SQL)** does not use the traditional table structure of an SQL database. This stores data in flexible formats like documents and is designed to handle a wide variety of data types and structures. It can manage large volumes of unstructured or semistructured data. NoSQL databases are useful for applications that require high flexibility, such as real-time web applications.
- A **data warehouse** integrates data from various sources and stores it in a combined manner (Amazon Redshift is an example). It is a specialized database optimized for analysis and reporting rather than transaction processing. A data warehouse is designed to perform complex queries and data analysis quickly and efficiently.
- A **data lake** stores large amounts of raw data in their original format until the data are needed. A data lake can handle structured, semistructured, and unstructured data (examples include Apache Hadoop and Amazon S3). A data lake is particularly useful for big data analytics.

An important database process is **data retrieval**, which involves obtaining specific information from a database or storage system. It queries the database using methods such as SQL in relational databases to extract needed data quickly and efficiently. The purpose of data retrieval is to access information for analysis, reporting, or decision-making, making it an essential aspect of effective data management. A technique used to improve the speed of data retrieval operations in a database is **indexing**. By creating an index, a database can quickly locate and access data without having to scan the entire table. The most common type of index is the **B-tree index**, which maintains a balanced tree structure (a tree structure where all branches are kept roughly the same height), providing efficient insertion, deletion, and lookup operations.

LINK TO LEARNING

Learn more about how a B-tree index (https://openstax.org/r/109BTreeIndex) provides sorted data and allows for efficient searching and access, plus variations in types of B-tree indexes.

Another type is the **hash index**, which uses a hash function to map data to a fixed-size table. Hash indexes are ideal for equality searches but are less efficient for range queries (Table 3.2). For example, a hash index works well when searching for something specific, like "Find Customer ID = 342678," because it can quickly locate that exact ID. But it's not as good for tasks like "Find all customers with IDs between 2000 and 2200," since hash indexes do not keep data in order, making range searches slower.

Number	First Name	Last Name	Country
342678	Chris	Assam	USA
675309	Taylor	Tan	Australia
649568	Anthony	Ray	Mexico

Table 3.2 Customer Data in a Hash Index Hash indexing can map values to locations in tables but are inefficient when looking up range values.

A **bitmap index** uses 0s and 1s to show where a value is in a database. It's great for columns with only a few options, like "Yes/No" or "Rent/Own/Neither," and facilitates quick searching. Bitmap indexes are efficient for columns with a limited number of distinct values and are often used in data warehouses for complex queries on large datasets. Full-text indexes organize words in text fields to make it easier and faster to search for specific words or phrases.

Data retrieval techniques (Table 3.3) ensure that data can be efficiently retrieved, processed, and utilized for different applications, ranging from simple queries (such as using SQL to pull specific data, like finding all customers from a certain city) to complex data analysis and mining (for example, finding patterns in large datasets, like discovering what products people buy together).

Retrieval Technique	Description
SQL	Used to query and manipulate data in relational databases
NoSQL database	Handles unstructured and semistructured data with specific query languages

Table 3.3 Data Retrieval Techniques There are different ways to retrieve data, from simple SQL queries to quickly finding records to indexing for faster searches.

Retrieval Technique	Description
Full-text search engine	Indexes text data to enable complex search queries
API	Provides access to data from web services and applications using HTTP methods
File-based retrieval	Retrieves data stored in files using programming languages
Web scraping	Extracts data from websites using tools
Data warehousing	Aggregates data from multiple sources for complex queries and analytics
Indexing	Improves data retrieval speed by creating quick lookup structures
In-memory data grid	Stores data in random access memory for faster access, supporting distributed caching and querying
Metadata search	Retrieves data based on descriptive information
Data mining	Extracts patterns and knowledge from datasets

Table 3.3 Data Retrieval Techniques There are different ways to retrieve data, from simple SQL queries to quickly finding records to indexing for faster searches.

SQL consists of the following:

- Database: a collection of related data
- Table: a collection of related data entries consisting of columns and rows
- Column: a vertical entity in a table that contains all information associated with a specific field
- Row: a horizontal entity in a table that contains a single record

Basic SQL commands include CREATE TABLE, INSERT, SELECT, UPDATE, and DELETE for managing databases (Table 3.4):

- CREATE TABLE: makes a new table with specified columns and data types
- INSERT INTO: adds new data to a table
- SELECT: retrieves data from a table
- UPDATE: changes existing data in a table
- DELETE: removes data from a table

SQL Command	Example
Creating a table	`CREATE TABLE customers ( id INT PRIMARY KEY, name VARCHAR(50), age INT, country VARCHAR(50) );`
Inserting data into a table	`INSERT INTO customers (id, name, age, country) VALUES (1, 'John Doe', 30, 'USA');`
Retrieving data selecting all columns	`SELECT * FROM customers;`
Retrieving data selecting specific columns	`SELECT name, country FROM customers;`
Filtering results	`SELECT * FROM customers WHERE country = 'USA';`
Using logical operators	`SELECT * FROM customers WHERE country = 'USA' AND age > 25;`
Updating data	`UPDATE customers SET age = 31 WHERE id = 1;`
Deleting data	`DELETE FROM customers WHERE id = 1;`

Table 3.4 Basic SQL Commands Key SQL commands include CREATE TABLE to make tables, INSERT INTO to add data, SELECT to retrieve data, UPDATE to change data, and DELETE to remove data. These commands are essential for managing any database (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license).

A DBMS is a set of software programs that let users create and maintain databases. It provides a way to interact with the data, ensuring data are stored systematically in a structured and consistent way, making them easy to access, manage, and efficiently retrieve. DBMSs offer many advantages, such as improved data integrity and consistency, reduced redundancy, control over data independence, trusted security and access protocols, and overall management and backup protections.

Data integrity refers to the accuracy and consistency of data stored in a database. A DBMS enforces rules and constraints such as primary keys. A **primary key** is a unique identifier for each data entry in a database table. It ensures that no two rows in the table have the same value for this key, enforcing data integrity. It cannot have duplicate or null values. For example, in a “Customers” table, “CustomerID?” could be the primary key because it gives every customer a unique ID. Constraints like primary keys prevent incorrect data entry and maintain the integrity of the data over time. For example, a DBMS can enforce that an email field must contain a valid email format, preventing incomplete entries.

A DBMS also supports **data consistency**, ensuring that data remain consistent and accurate across the database. It enforces consistency through ACID properties in transactions, meaning that all operations within a transaction are completed successfully, and the database remains in a consistent state. For example, transferring money from one account to another involves two steps: debiting one account and crediting another. Both steps must be completed in the correct order, ensuring consistency.

A DBMS reduces **data redundancy**, or the duplication of data, to save space and prevent inconsistencies. Using normalization, DBMS structures the data in a way that reduces redundancy. For example, instead of storing customer details in multiple places, they are stored in only one place and referenced as needed. A DBMS also allows for **data independence**, meaning that data can be structured without affecting the programs that use it. This works because DBMSs use a schema, which shows the structure of the data separately from how the data are stored.

Protection of data from unauthorized access to ensure data privacy is considered data security. A DBMS provides robust security features like user authentication (verifying a user's identity before granting access to a system), access controls, and encryption (arranging data into an unreadable code that can only be read with a key). For instance, only authorized users can access certain data in a company's database. Concurrent access allows multiple users to access and modify the data simultaneously and without conflicts. A DBMS uses a locking mechanism to ensure that multiple operations can occur simultaneously without data corruption. For example, while one user is updating a record, another user can still view the data without interruption. Backup and recovery allow data to be backed up and restored after a failure or loss. A DBMS provides automated backup and recovery solutions.

Database Design Techniques

Database design is the process of organizing data according to a database model, which indicates how to structure the data and how the data are stored and connected. A well-designed database will store and retrieve data efficiently and ensure the data are accurate and accessible. Design involves understanding the data needs of an organization and structuring the data to minimize redundancy and maximize performance.

A database modeler designs and plans how a database will work. This person figures out what data are required to create the structure (like tables and relationships, often called entity relationship diagrams), and makes sure the database is efficient, secure, and easy to use. They also work with developers and administrators to set it up and keep it running smoothly by following specific constraints. Constraints are rules applied to database tables to ensure data integrity and reliability (for example, entity constraints that ensure each table has a primary key). A **referential constraint** maintains relationships between tables, making sure that a foreign key in one table matches a primary key in another table. This ensures that the relationships between records are consistent and eliminates any **orphaned record**, or a record that references another record that no longer exists. A **check constraint** specifies the values that can be entered into a column. For example, a check constraint can ensure that the values in an age column are always positive, or that the status column only contains predefined values like "Active" or "Inactive."

A database design usually proceeds through three stages: conceptual, logical, and physical design. Prior to these, the designer must conduct a **requirements analysis**, which is a study of how a business operates to determine what data should be stored and how the data should be used. It helps in understanding what users need from the database. This involves studying how the business operates to determine what data should be stored and how the data should be used.

Next, the **conceptual design** creates a simple model of the data, focusing on what is needed and how it's connected. It involves identifying key items like customers or products (entities), their details like names or prices (attributes), and how they are related, such as "customers place orders." An ERD is often used to map this out clearly. This ensures the database fits the business or application needs. Once the concept is determined, the next step is to turn the initial models into a more detailed a **logical design**, which defines tables, columns, primary keys, and foreign keys. A **foreign key** is a column or set of columns in one table that establishes a relationship with the primary key in another table. These keys are used to maintain referential integrity between the two tables, ensuring that the value in the foreign key column corresponds to an existing value in the referenced table. Finally, the **physical design** translates the logical design into a physical structure (via actual implementation in the database) that the DBMS can use. This involves choosing data types, indexing strategies, and planning for storage.

The database modeler also needs to attend to these needs during the design:

- Schema refinement: Making sure the database design is free of issues such as storing the same data in multiple places to save space.
- Data integrity and validation: Ensuring the data remain accurate. This is achieved through constraints (rules applied to database columns to ensure data integrity and accuracy) and stored procedures (such as prewritten SQL programs stored in the database that perform specific tasks) that enforce business rules and validate the data.
- Documentation: Creating detailed documentation for developers, administrators, and users.
- Prototyping and iterative refinement: Building a prototype of the database, testing it, and refining the design based on feedback and performance results. This helps catch issues early and ensures the design meets user needs.
- Security design: This protects database data by managing who can access it, encrypting sensitive info, and keeping track of activity. It ensures the data stay safe and recoverable.
- Maintenance: Ensuring the database can be maintained over time.

A **functional dependency** describes how one piece of data relates to another within a table. For example, in a table of employees, entering the employee ID should provide you with their name and address. One of the ways of checking the dependencies is **normalization** in which data are organized and stored only once to eliminate the duplication of data. Normalization occurs across three stages:

1. First normal form (1NF): Ensures each column contains atomic, indivisible values. Each column has single, simple values, and rows are unique. For example, multiple phone numbers do not appear in one cell—each number gets its own row.
2. Second normal form (2NF): Ensures the database is in 1NF and that all nonkey columns depend on the whole primary key. For example, in a table with OrderID and ProductID as the key, Quantity must depend on both, not just one.
3. Third normal form (3NF): This form ensures the database is in 2NF and that all columns are dependent only on the primary key.

For systems analysts, understanding normalization is key when working with relational databases. Normalization helps organize data to avoid problems like duplicate records or errors. However, it's important for a systems analyst to know when to balance normalization with performance needs.

In cloud environments or large systems, sometimes **denormalization**, or the addition of redundant data, is used to make things run faster and meet specific requirements. Consider a systems analyst managing a database for an online store. The database has two tables: one table is Customers (with customer information like name and address), and the other table is Orders (and includes details about each order). Normally, these tables are kept separate and are linked by a customer ID. This keeps the data clean—if a customer updates their address, you only need to change it in one place. But if the store is busy, joining tables every time someone checks an order can slow things down. To fix this, the analyst might denormalize the database by combining some tables to allow data retrieval to occur more quickly. Instead of keeping customer information separate, the organization could decide to store the customer's name and address directly in the Orders table. While this makes it faster to retrieve orders, if the customer changes their address, it will have to be updated in multiple places. This is how analysts balance keeping the data clean with making the system run more quickly.

Table 3.5, Table 3.6, and Table 3.7 show how a database progresses through the first, second, and third normal forms (1NF, 2NF, 3NF) using tables for an online store's customer and ordering data.

Beginning Data				
OrderID	CustomerName	Address	Products	TotalPrice
101	John Doe	123 Main St	Shirt, Shoes	$75
102	Jane Smith	456 Oak Ave	Hat, Bag	$50
103	John Doe	123 Main St	Jacket, Sunglasses	$120
First Normal Form (1NF)				
OrderID	CustomerName	Address	Product	TotalPrice
101	John Doe	123 Main St	Shirt	$75
101	John Doe	123 Main St	Shoes	$75
102	Jane Smith	456 Oak Ave	Hat	$50
102	Jane Smith	456 Oak Ave	Bag	$50
103	John Doe	123 Main St	Jacket	$120
103	John Doe	123 Main St	Sunglasses	$120

Table 3.5 First Normal Form (1NF) To begin, the data might have multiple values in one field. In 1NF, the products are separated into individual rows to ensure there is only one value per field.

Second Normal Form (2NF)—Orders		
OrderID	Product	TotalPrice
101	Shirt	$75
101	Shoes	$75
102	Hat	$50
102	Bag	$50

Table 3.6 Second Normal Form (2NF) In 2NF, partial dependencies are removed by splitting the data into two tables: one for Orders and another for Customers.

Second Normal Form (2NF)—Orders		
103	Jacket	$120
103	Sunglasses	$120
Second Normal Form (2NF)—Customers		
CustomerID	CustomerName	Address
1	John Doe	123 Main St
2	Jane Smith	456 Oak Ave

Table 3.6 Second Normal Form (2NF) In 2NF, partial dependencies are removed by splitting the data into two tables: one for Orders and another for Customers.

Third Normal Form (3NF)—Orders			
OrderID	Product	TotalPrice	CustomerID
101	Shirt	$75	1
101	Shoes	$75	1
102	Hat	$50	2
102	Bag	$50	2
103	Jacket	$120	1
103	Sunglasses	$120	1
Third Normal Form (3NF)—Customers			
CustomerID		CustomerName	
1		John Doe	
2		Jane Smith	
Third Normal Form (3NF)—Addresses			
AddressID		Address	

Table 3.7 Third Normal Form (3NF) In 3NF, transitive dependencies are removed by creating a separate Addresses table.

Third Normal Form (3NF)—Orders	
1	123 Main St
2	456 Oak Ave

Table 3.7 Third Normal Form (3NF) In 3NF, transitive dependencies are removed by creating a separate Addresses table.

Studying the three models of database design—conceptual, logical, and physical—is important because they help ensure a database is well planned, functional, and efficient. A conceptual model is a high-level outline of what data the database will hold and how that data relate to each other. Think of it as the blueprint of an organization's database, often visualized using ERDs. The physical model describes how the database will be implemented on a specific database management system. It considers technical aspects like storage, indexing, and performance. A logical model takes the conceptual model and adds more detail. It includes data types, indexing, and storage specifics.

Gathering, Organizing, Curating, and Processing Data

Data serve as a cornerstone for decision-making and innovation across various disciplines, ranging from scientific research to business management. Whether engaged in academic research, business operations, or personal projects, knowing how to effectively gather, organize, curate, and process data is imperative.

Gathering Data

The gathering data stage includes identifying data sources, data collection methods, and tools for data collection. Data sources can be categorized into primary and secondary sources. Primary data refers to data collected firsthand through methods such as experiments, surveys, or direct observations. Secondary data include data previously collected by other researchers or organizations and are accessible through books, articles, and other databases. The choice of data collection method depends on the research objectives and the nature of the data required. Table 3.8 lists some considerations and examples for collecting primary data.

Method	Description	Who Uses Them	When to Use Them	Example
Surveys and questionnaires	Useful for collecting data on opinions or preferences used to gather information from large groups of people can be conducted online, over the phone, or in person	Public health officials and educational researchers	When collecting standardized data, such as opinions or behaviors, from many participants	A school district might survey parents to assess satisfaction with online learning programs
Experiments	Employed to obtain specific data points under controlled conditions to test hypotheses by manipulating variables and observing the outcomes	Scientists and medical researchers	When determining cause-and-effect relationships under controlled conditions	A researcher might test what level of a drug is needed to produce a medical effect.
Observations	Involve recording data based on direct observation by watching behaviors or events	Educators and psychologists	When studying real-life interactions or behaviors as they occur	An educator might observe students during group activities to assess collaboration skills.
Interviews	Involve one-on-one conversations that explore a participant's experiences or opinions in depth	Social scientists, psychologists, and health-care professionals	When the researcher needs rich, detailed responses or when exploring sensitive topics	A researcher studying stress among health-care workers might conduct interviews to capture personal stories and insights.

Table 3.8 Primary Data Collection There are several methods for gathering primary data. The source and type of data influence which method is most appropriate.

Organizing Data

Proper data organization ensures that data can be easily manipulated and analyzed in tabular, hierarchical, and graphical formats. Tabular format organizes data in rows and columns, facilitating sorting and filtering; hierarchical format structures data in a treelike format, suitable for nested information; and graphical format represents data as nodes and edges, ideal for depicting relationships and networks.

Implementing best practices in data management enhances data integrity and usability. Using consistent naming conventions helps avoid confusion by ensuring files and variables are clearly and uniformly named. Version control is essential for keeping track of different iterations of datasets, making it easier to manage changes over time. Regular backups can prevent data loss, ensuring that data remain safe and accessible.

Curating Data

Curating data involves several important steps to ensure its accuracy and reliability. Data cleaning is the first step, which includes handling missing values by deciding whether to flag or remove incomplete records, removing duplicates to ensure each record is unique, and standardizing formats for dates, units, and other data points. Data transformation is the process of making data more suitable for analysis through normalization. Ensuring data quality is the final step and involves making sure the data are accurate, consistent, complete, and timely. This is done by checking that data entries are correct and precise, verifying uniformity across different sources, ensuring no crucial data are missing, and using the most up-to-date data available.

Processing Data

Processing data involves various techniques and tools to analyze and visualize information effectively. Descriptive statistics—like mean, median, mode, and standard deviation—summarize data, while inferential statistics use hypothesis testing and confidence intervals to draw conclusions about a population. Machine learning algorithms, such as regression and classification models, provide predictive analysis. Tools like Microsoft Excel and Google Sheets are useful for basic analysis, while advanced statistical software like R, SPSS, and SAS offer capabilities that are more sophisticated. Programming languages like Python, with libraries such as Pandas and R, are powerful tools for data manipulation and analysis. Effective data visualization enhances understanding through charts and graphs, such as bar charts, line graphs, and scatterplots, while advanced tools like Tableau and Microsoft Power BI offer more complex visualization options. Dashboards provide interactive platforms for real-time data monitoring and decision-making.

Data Security and Access Control

Database security involves protecting the database against unauthorized access and potential threats. Measures include implementing strong access controls, using encryption, performing regular security audits, and monitoring for suspicious activities (you will learn more about these topics in Chapter 5 Information Systems Security Risk Management and Chapter 6 Enterprise Security, Data Privacy, and Risk Management.

User management includes creating, managing, and monitoring database user accounts. Proper user management ensures that only authorized personnel have access to specific data, and roles and permissions are assigned based on the principle of least privilege, which is giving a user, system, or process only the minimum access or permissions needed to perform their specific tasks. Ensuring that database transactions are processed efficiently is essential. This includes maintaining data consistency and integrity through ACID properties. Proper transaction management helps prevent issues like data corruption and ensures that operations are completed fully or not at all.

ETHICS IN IS

Structured Query Language Injections

In 2011, Sony faced a major data breach in their PlayStation Network when attackers used SQL injection to exploit weaknesses in their systems. An SQL injection is a type of security vulnerability that occurs when an attacker is able to insert or manipulate SQL queries within a web application's input fields. It allows the attacker to retrieve sensitive data from the database, such as usernames, passwords, or financial information. This can happen when the application fails to properly sanitize user input before incorporating it into an SQL query, allowing the attacker to execute malicious SQL commands. This gave hackers access to sensitive customer information, including credit card numbers. The incident showed how critical it is for organizations to secure their databases and control access to prevent such attacks. Views and authorization are critical for preventing SQL injection attacks, where hackers use harmful inputs to access or manipulate database data.

To prevent SQL injection, the following practices are recommended:

- Views only show users the data they need, hiding sensitive information.
- Authorization controls ensure users can only access what their role allows.
- Parameterized queries treat user inputs as data, not code, which allows for blocking of harmful code.
- Input validation checks and cleans user inputs to prevent attacks.
- Stored procedures standardize input handling, reducing vulnerabilities.
- Regular security checks help identify and fix weaknesses.

Using these practices together makes databases much safer from SQL injection attacks.

One important user management procedure is **access control**, which is the security-driven restriction of access to ensure that only authenticated users are able to interact with specific resources. There are four common access control models: mandatory, discretionary, role-based, and privileged (Table 3.9):

Mandatory access control (MAC) is highly restrictive and typically used in government and military environments. In MAC, a central authority based on security clearances assigns access permissions to individuals working for the organization. For example, individuals with the necessary top-secret clearance are the only ones who can access a top-secret document in a military database. Users cannot alter permissions, ensuring strict compliance with the organization's security protocols.

Discretionary access control (DAC) allows resource owners to decide who can access their data. For instance, if you own a file on your company's shared drive, you can grant or deny access to other colleagues. While this model offers flexibility, it can lead to security risks if not managed carefully. For example, if an employee shares a sensitive document with a contractor without proper vetting, it could lead to unauthorized access.

Role-based access control (RBAC) assigns permissions based on a user's role within an organization. For example, an employee in the human resources department is given access to payroll information and employee records, while someone in IT is granted access to system configurations and network settings. This model simplifies management by grouping permissions based on roles rather than individual users, making it easier to update access as roles change. For instance, when a junior developer gets promoted to a senior developer, their role-based access can be updated to include additional system privileges.

Privileged access management (PAM) focuses on controlling and monitoring access for users with elevated permissions, often referred to as privileged accounts. For example, system administrators may have the ability to install software, configure network settings, and access sensitive data. PAM solutions ensure that these high-level permissions are used appropriately and securely by providing tools for monitoring, auditing, and managing access. For instance, a PAM system can track and log every action taken by an administrator—such as changes to firewall settings—ensuring accountability and security.

Table 3.9 summarizes some of the pros and cons of each of these four access control models.

Access Control Model	Advantages	Disadvantages
Mandatory access control (MAC)	• Provides robust security and restricts access permissions • Reduces the risk of unauthorized access	• Can be complex to implement and manage • Not easily adaptable to changing business needs
Discretionary access control (DAC)	• Resource owners have the freedom to grant access • Easier to set up and manage for smaller environments	• Increased risk of unauthorized access due to the potential for users to inadvertently grant permissions • Can lead to inconsistent application of security policies across the organization
Role-based access control (RBAC)	• Simplifies management by grouping permissions • Easier to manage as the organization grows	• Can lead to a large number of roles that need to be managed • Not as adaptable to temporary changes in roles or duties
Privileged access management (PAM)	• Focuses on controlling and monitoring high-level permissions • Provides detailed logging and auditing of activities	• Can be complex to implement and manage, requiring significant resources and expertise • May lead to frustration among users if access is too restricted

Table 3.9 Access Control Models Access control models such as MAC, DAC, RBAC, and PAM each have their own advantages and disadvantages. They can be adapted for dynamic access control, especially with the shift to remote and blended workforces.

Choosing the right access control model for an organization can be challenging. A small defense subcontractor might need to implement MAC systems for its entire operation to meet strict security requirements determined by government regulations or classified contracts. In contrast, a prime contractor, which is a large organization managing multiple subcontractors, can use a more nuanced approach, reserving MAC systems for its most sensitive operations, such as handling classified defense projects.

Some industries commonly use role-based access controls, so that different system users (such as employees, managers, or suppliers) only have access to specific information. For example, a manager might have access to employee schedules and inventory records, while a cashier may only have access to the point-of-sale system.

Comparing Database Management Systems

When working with database management systems, it is important to understand the different types available and how they are used in various applications. We'll focus on comparing three major types: relational, object oriented, and NoSQL. Learning the strengths and limitations of each provides insight into when and why to use them, based on specific project needs.

A **relational database management system (RDBMS)** is a database management system that stores and organizes data in a structured way using tables. Each table represents an entity, and each row in the table represents a record of that entity, while columns represent the attributes of the entity. An RDBMS requires a predefined schema, which is a document that defines the structure of the data in terms of tables and the relationships between them. Relationships between tables are established using foreign keys, which reference primary keys in other tables, ensuring referential integrity. The RDBMS enforces data integrity through constraints such as primary keys, foreign keys, unique constraints, and checks. The SQL is the standard language used to interact with an RDBMS for defining, querying, and manipulating data. Additionally, an RDBMS adheres to ACID properties to ensure reliable transaction management. Normalization is a key practice in an RDBMS, aimed at reducing data redundancy and improving data integrity by organizing data into multiple related tables. As an example of an RDBMS, a university stores student records in tables, with a predefined schema that organizes data into entities like “Students,” “Courses,” and “Grades,” linked by relationships. The structure ensures data consistency and simplifies reporting.

Object-oriented programming principles are fundamental concepts that guide the design and implementation of programs in object-oriented languages like Java, Python, and C++. An **object-oriented database management system (OODBMS)** stores data in the form of objects, similar to the way data are represented in object-oriented programming languages. Each object includes both data, in the form of attributes, and behavior, in the form of methods. This approach allows for a more direct mapping between the database and the application’s data model, facilitating complex data representations and relationships. An OODBMS supports classes, inheritance, polymorphism, and encapsulation, enabling the creation of complex data types and relationships that mirror real-world entities more closely. The schema in an OODBMS is defined using object-oriented concepts, and objects can contain references to other objects, enabling rich, interconnected data structures. Querying in an OODBMS is typically done using object query languages, which are designed to operate on objects and their relationships. An OODBMS is particularly well suited for applications requiring a complex data model—such as computer-aided design (CAD), computer-aided manufacturing, multimedia, and telecommunications—that requires efficient handling of complex data types and relationships efficiently. As an example of an OODBMS, a CAD software company can use an OODBMS to store data about three-dimensional models. Each model is an object containing data and methods reflecting real-world design elements.

A **NoSQL database management system** is a type of database that provides a mechanism for storing and retrieving data that is not based on the traditional relational database model. They are built to handle large amounts of data, high-speed data processing, and diverse data types. They offer scalability, flexibility, and performance, making them ideal for modern applications that manage big data and real-time web applications. Because a NoSQL DBMS does not require a fixed schema, they permit rapid or ad hoc changes to data structures. They also support distributed computing, which helps manage large-scale data across multiple servers. NoSQL databases come in various types, including key-value stores, document-oriented databases, column-family stores, and graphical databases, each tailored to specific types of data and use cases. Key-value stores organize data by associating them with a unique identifier (the key) and its corresponding value, which can be a simple string or a complex object. The simplicity of key-value stores makes them very fast for certain types of tasks, particularly those involving straightforward data access patterns. They are perfect for applications like caching, session management, and real-time data analytics. A document-oriented database, which has a flexible schema, works well with a NoSQL database management system. Document-oriented databases store data in the form of documents, usually using formats like JSON, BSON (binary JSON), or XML. Each document contains a self-contained data structure made up of fields and values, which can include nested documents and arrays. This flexible schema allows for storing complex data structures without needing a predefined schema, making it easy to adapt to changes in data requirements over time. Document-oriented databases are great for applications that need hierarchical data storage, such as content management systems, e-commerce platforms, and real-time analytics. As an example of NoSQL databases, a social media platform uses a document-oriented NoSQL database to store user profiles, posts, and comments. The flexible schema easily adapts to new features, like adding reactions or multimedia support.

3.2 Practical Applications of Database Design and Management

Learning Objectives

By the end of this section, you will be able to:

- Describe the design process and structure for a database management system
- Discuss the various applications of database management systems for different industries

Database design and management are important for businesses because they help store, organize, and retrieve data efficiently. A well-designed database design ensures data are accurate, secure, and easy to access. This is important in many information systems in the enterprise, such as customer relationship management, financial systems, and health-care information systems. These systems rely on databases to function correctly and support day-to-day operations of a company or organization.

In e-commerce, databases help manage product inventory, track customer orders, and analyze sales. For example, companies like Amazon use complex databases such as DynamoDB, a fully managed NoSQL database, to handle millions of transactions daily and provide personalized recommendations to customers. These databases help keep track of stock, update customers on their orders, and tailor marketing strategies to individual preferences, leading to better customer satisfaction and increased sales.

The health-care industry serves as a strong example of how an industry benefits from well-designed databases. Electronic health records (EHR) database systems store patient information, medical histories, and treatment plans. The Epic Systems EHR system is the most widely used system in the United States, has the largest hospital EHR share in the world, and provides the top healthcare app, MyChart.[2] An EHR system makes it easier for health-care providers to access patient data, coordinate care, and improve the quality of services. Databases also help integrate different health information systems, like lab results and imaging studies, giving a complete view of a patient's health. Effective health-care database management ensures patient data are kept confidential and secure and follows laws like HIPAA. Almost 78 percent of office-based doctors and 96 percent of hospitals in the United States now use EHR systems.[3] While smaller practices often struggle with higher costs and less support, EHRs are becoming more common across health care, helping to improve patient care and streamline operations.

Database Design

There are two fundamental stages of database design—logical and physical. Logical design involves creating a blueprint of the database that outlines the structure *without* considering how it will be physically implemented. This stage includes defining entities, their attributes, and relationships, often using tools like ERDs. The goal is to ensure that the database model aligns with business requirements and eliminates redundancies, such as duplicate records or repetitive fields. Physical design focuses on how the database will be built on a specific DBMS. It includes selecting data types, indexing strategies, and storage methods to optimize performance and storage. The transition from logical to physical design is essential as it translates a theoretical model into a practical, efficient database.

Database design needs to take into consideration the data and the data life cycle. As Figure 3.2 illustrates, the **data life cycle** includes the stages that data undergo from collection to deletion, ensuring data remain accurate, accessible, and valuable throughout their life cycle. It begins with data collection where raw data are gathered from various sources, with the goal of capturing accurate and relevant information for future use. Next, data storage involves saving this information in a database for easy access and management, ensuring it is organized and can be retrieved efficiently. Processing follows, and data are cleaned, transformed, and

2 Giles Bruce and Naomi Diaz, "50 Things to Know about Epic," *Becker's Hospital Review*, October 17, 2024, https://www.beckershospitalreview.com/ehrs/50-things-to-know-about-epic.html

3 "National Trends in Hospital and Physician Adoption of Electronic Health Records: Health IT Quick-Stat #61," Assistant Secretary for Technology Policy, Office of the National Coordinator for Health Information Technology, 2021, accessed January 28, 2025, https://www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records

organized to prepare the data for analysis, ensuring data quality and usability. During the data analysis phase, data are examined by stakeholders to extract useful insights that inform decision-making, revealing patterns, trends, and correlations valuable for strategic planning. Finally, data are either archived for future reference or deleted if no longer needed, maintaining a clean and efficient database environment.

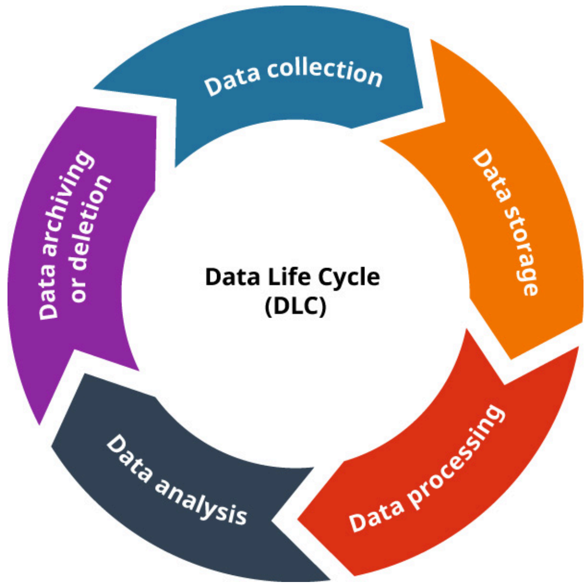


Figure 3.2 The data life cycle processes are interconnected and continuous. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Database system design should proceed through several steps:

1. Defining requirements
2. Designing the structural components
3. Ensuring performance capabilities
4. Creating a positive user experience
5. Planning for smooth integration with existing systems

The first step in database design is to gather and define the system requirements. This involves understanding the needs of the users and the objectives of the database. Requirements are categorized as functional, detailing what the database should do, and nonfunctional, specifying performance criteria such as speed, reliability, and security. Clear and comprehensive requirements ensure that the database system meets user expectations and business goals, providing a solid foundation for the design process.

Once the requirements are defined, the next step is to map out the system's structure and architecture. Diagrams can illustrate how different components of the system interact with each other. These may include software modules, hardware components, network infrastructure, and data storage solutions. A clear architecture helps plan the implementation and ensures that all parts of the system work together harmoniously, facilitating efficient and effective design.

A critical aspect of database system design is ensuring that the database performs efficiently and can scale to handle increasing loads. This involves selecting appropriate technologies, optimizing algorithms, and designing for concurrency and parallel processing. Scalability ensures that the database can grow and adapt to higher demands without significant performance degradation. This is particularly important for databases expected to handle large volumes of data or high user traffic, ensuring long-term viability and performance.

The design process also focuses on creating a positive user experience. This includes designing intuitive user interfaces, ensuring fast response times, and providing clear results to users.

Finally, database design must ensure smooth integration with existing systems. This might involve interfacing with legacy systems, using standardized protocols for communication, and ensuring data compatibility. Successful integration minimizes disruptions and allows for seamless operation across different platforms and technologies, enhancing the overall functionality and efficiency of the database system.

Steps for Determining the Design and Structure for a Database Management System

To determine the design and structure for a DBMS, consider the process of designing a library management system. Imagine you're tasked with designing a library management system for a local library. The system must handle book inventories, track borrowings and returns, maintain member records, and generate reports. This scenario will guide you through the design process using a structured task list.

1. Requirement analysis. The first step is to gather and analyze user requirements. After consulting with library staff and stakeholders, you identify the following criteria:
   - Store information about books, including
     - title,
     - author,
     - International Standard Book Number (ISBN) (a unique thirteen-digit code used to identify a book),
     - edition, and
     - availability status.
   - Maintain member records with details like
     - name,
     - membership ID,
     - contact information, and
     - borrowing history.
   - Track lending and returns, including
     - due dates and
     - fines for overdue books.
   - Generate reports such as
     - book inventories,
     - popular books, and
     - member activity.
   - Support user authentication with roles for librarians and regular members.
2. Feasibility study. Next, you conduct a feasibility study to ensure the project is viable:
   - Technically, the project is feasible with the available tools, including an RDBMS like MySQL.
   - Economically, the library has allocated a sufficient budget. The budget is the amount of money reserved for the project and was decided by the finance committee. If the budgeted amount is not enough, they could apply for grants, shift funds from other areas, or adjust the project to focus on the most important parts.
   - Legally, there are no significant concerns, but data privacy for member records must be ensured.

   From the first two steps, you determine that the project is feasible and worth pursuing.
3. System specification is based on the requirements, so you define the DBMS specifications:
   - The system will be a web application with a MySQL database back end. The **back end** is the part of a software application that handles data, logic, and operations, supporting what users interact with on the front end. The **front end** is the part of a software application that users interact with, including the design and user interface.
   - The system will contain modules for
     - book management,

        - member management,
        - lending and return tracking, and
        - reporting.
    - User roles will be implemented to distinguish between librarians and regular users.
    - The application will be accessible via the library's internal network.

4. Logical design is the next phase where you will create data models and define the DBMS architecture. You design ERDs to represent the following entities and their relationships:
    - Book attributes include
        - book ID,
        - title,
        - author,
        - ISBN,
        - genre, and
        - availability.
    - Member attributes include
        - member ID,
        - name,
        - contact information, and
        - membership date.
    - Lending attributes include
        - loan ID,
        - book ID,
        - member ID,
        - loan date,
        - due date, and
        - return date.

   The relationships between these entities are established, such as a member can borrow multiple books, and a book can be borrowed by multiple members over time.

5. Physical design. In this phase, you plan the database schema based on the logical design. You define the tables, columns, and data types. Table 3.10, Table 3.11, and Table 3.12 represent the attributes and data types for books, member, and lending tables.

Attribute	Data Type
BookID	Primary Key - Integer
Title	CHAR
Author	CHAR
ISBN	CHAR
Generation	CHAR
Availability	BOOLEAN

Table 3.10 Books Table First, the attributes and data types for the book table are defined.

Attribute	Data Type
MemberID	Primary Key - Integer
Name	VARCHAR
ContactInfo	VARCHAR
MembershipDate	DATE

Table 3.11 Member Table Next, the attributes and data types for the member table are established.

Attribute	Data Type
LendingID	Primary Key - Integer
BookID	Foreign Key - Integer
MemberID	Foreign Key - Integer
LoanDate	DATE
DueDate	DATE
ReturnDate	DATE

Table 3.12 Lending Table Finally, the attributes and data types for the lending table are defined.

You also consider indexing strategies to optimize query performance and storage methods to ensure efficient data retrieval.

6. Prototyping is the next step for developing a library management system, and you'll focus on key functionalities like
   - book search,
   - member registration, and
   - borrowing transactions.

   You then present this prototype to the library staff for feedback. The prototype is well received, and they suggest adding a feature to notify members about due dates via email.
7. System integration is the next step as you integrate various components of the DBMS, ensuring that the web application interfaces correctly with the MySQL database. You also integrate the email notification feature suggested by the library staff, using an SMTP server to send due date reminders to members.
8. Testing is conducted to ensure the DBMS works as expected. Individual functions are verified by a **unit test**, an **integration test** checks the interaction between modules, and a **system test** evaluated the overall functionality. To ensure the system meets the needs of the end users, **user acceptance testing** is performed.
9. Documentation is an important step as you create comprehensive documentation, including user manuals

for librarians and technical documentation for developers. The user manual covers how to

- manage books,
- register members,
- process loans and returns, and
- generate reports.

The technical documentation includes database schemas, API references, and deployment instructions.

10. Deployment on the library's internal network is a major step for your system. Software is installed on the server, the database is set up, and the application is configured. The library staff is trained to use the new DBMS.
11. Maintenance is provided to keep the system running smoothly. This includes
    - regular backups of the database,
    - updates to the software, and
    - support for any issues that arise.

Feedback from the library staff is continuously gathered to make further improvements to the system. By following these steps, you have successfully designed and implemented a database management system that meets the library's needs and enhances their operational efficiency.

Applications of Database Management Systems in Different Industries

Databases and DBMSs are used extensively across various industries. In health care, databases are used to store patient records, medical histories, treatment plans, prescriptions, and billing information. Common DBMSs used in health care include MySQL, PostgreSQL, Oracle Database, and MongoDB. These databases allow health-care providers to access patient data quickly and enhance the quality and coordination of care.

Electronic health record systems integrate various data points to give a comprehensive view of a patient's health status, aiding in better diagnosis and treatment. Health-care databases often use relational structures to ensure data integrity and support complex queries. Increasingly, cloud-based databases are being adopted for their scalability, flexibility, and compliance with data security regulations like HIPAA standards.

Financial institutions use databases for transaction processing, customer information management, account balances, loan processing, and investment portfolios. Common DBMSs used in the financial sector include Oracle Database, Microsoft SQL Server, and IBM Db2. Financial database management systems need to be highly reliable and secure to handle sensitive financial data and support real-time transaction processing. They enable efficient management of large volumes of transactions and customer data. Relational databases are favored in finance for their robustness and ACID properties, ensuring reliable transaction processing. Some institutions also use NoSQL databases for big data analytics and handling unstructured data.

In education, databases manage student records, course schedules, grades, and administrative data. Learning management systems like Moodle, Canvas, and Blackboard use databases to store course materials, assignments, and grades, facilitating online learning and tracking student progress. Educational institutions typically use relational databases for structured data such as student records and course information. Cloud-based databases are popular due to their scalability, ease of access, and ability to support large numbers of users, especially in remote learning scenarios.

Manufacturers use databases to track inventory levels, manage supply chains, monitor production processes, and maintain equipment logs. Examples of DBMSs in manufacturing include SAP HANA, Oracle Database, SQL Server, and MongoDB. Databases support efficient operations by providing real-time data on stock levels, production schedules, and maintenance needs, helping optimize manufacturing processes and inventory management. Both relational and NoSQL databases are used. Relational databases handle structured data like inventory lists and production schedules, while NoSQL databases manage large volumes of sensor data from IoT devices in smart manufacturing.

Additional key industries using databases for management and control include retailers that use databases for managing product catalogs, customer orders, and transaction records; logistics companies that use databases to optimize routes, manage deliveries, and track shipments; and telecommunication providers that use databases to manage customer accounts, billing information, and network performance data.

3.3 Mobile Database Development and Cloud Database Management Systems

Learning Objectives

By the end of this section, you will be able to:

- Explain the challenges in developing a mobile first design with a database
- Discuss the considerations for cloud-based databases and their architecture

Mobile database development continues to be in high demand, as more businesses look for scalable and efficient ways to support their business. Mobile application development is closely tied to database design because apps rely on databases to store, manage, and retrieve data (Figure 3.3). Most commonly, lightweight embedded database systems such as SQLite are used to store data locally.

During development, the database structure is designed to align with the app's features. For example, an e-commerce app might need tables for users, products, orders, and payments. Apps also connect to databases allowing for tasks like user login and real-time updates. A well-planned database ensures the app runs smoothly, stays fast, and supports all the features users depend on.

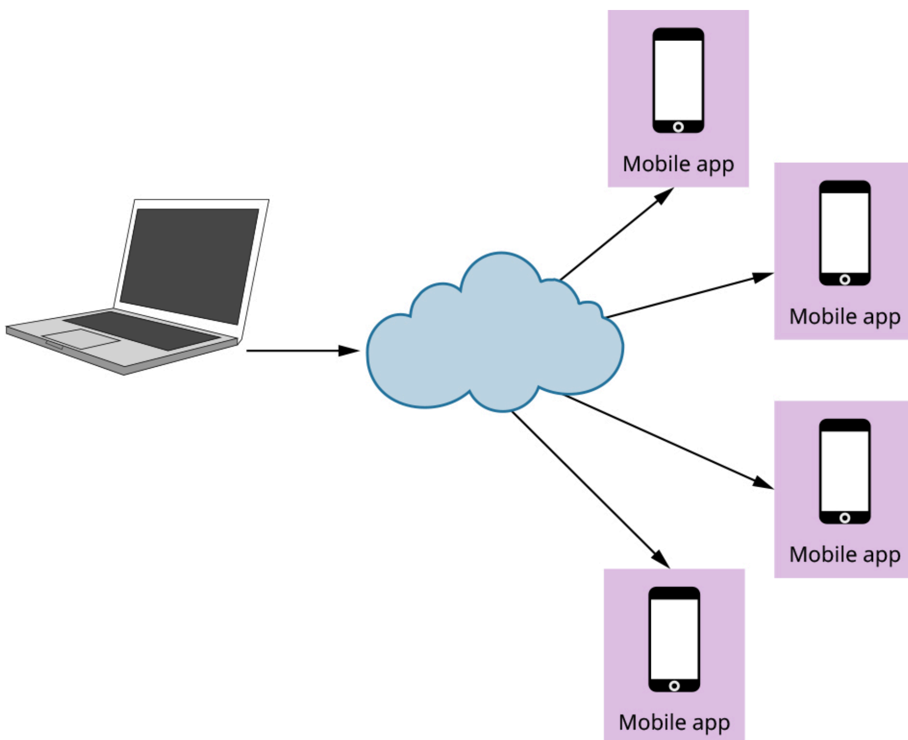


Figure 3.3 With the rise of mobile technology, accessing and interacting with data have changed, making strong back-end systems crucial for handling mobile users' needs. Cloud databases provide the infrastructure needed, offering real-time data access, scalability, and lower maintenance costs. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

In mobile app development, using cloud databases lets developers focus on user experience and app features without worrying about data storage and management. Services from providers like AWS, Google Cloud Platform, and Microsoft Azure offer databases designed for mobile apps. These databases ensure data synchronization across various devices, including smartphones, tablets, laptops, desktops, and IoT devices. For example, in a mobile app, real-time updates ensure a user's changes on a smartphone are immediately reflected on their tablet or desktop.

This integration also enables advanced features like offline data access, real-time updates, and easy app updates. For example, Firebase Realtime Database allows a mobile app to update users in real time, even when offline, by storing data locally and syncing it once the device reconnects.

Developing a Mobile-First Application with a Database

Mobile applications need to handle various forms of data input efficiently and accurately, ensuring that the collected information is stored securely and is easily retrievable. Some popular mobile apps include Google Drive and Google Docs for schoolwork and sharing files, Slack for group communication, and Spotify for streaming music.

Designing for Mobile Data Input

When designing a mobile application, one important consideration is how data are collected from users. As mobile devices have smaller screens and different input methods compared to desktops, optimizing forms and data entry interfaces for mobile use is necessary. Techniques such as responsive design, use of drop-down menus, autocomplete fields, and clear, concise instructions help ensure that users can enter data accurately. Validations should be implemented to check for correct data types, mandatory fields, and logical errors before the data are submitted, for example, ensuring an email field contains a valid email address format or a date field does not accept future dates when past dates are required. Many people use Instagram, Snapchat, and TikTok to stay connected with friends, and tools like Khan Academy and Quizlet are common for studying and learning.

Data Collection and Usage on Websites

Websites often collect user data through cookies, forms, and tracking technologies to personalize the user experience and for marketing purposes. These data are stored in databases and include information like user preferences, browsing history, and interaction patterns. By analyzing this data, websites can tailor content and advertisements to individual users, enhancing engagement and conversion rates. For instance, e-commerce sites use this data to recommend products based on previous searches and purchases. You've probably noticed how ads for products you recently liked or reviewed online show up in your search engine—this is a great example of how apps use data and databases to personalize the user experience and target customers.

Ensuring Data Cleanliness and Security

The term **data cleanliness** refers to the accuracy and consistency of data and the lack of duplicate, error, or missing information. Implementing validation checks at the point of data entry helps maintain data quality. Regular data audits and cleaning processes also remove duplicates, correct errors, and update outdated information.

Security is paramount, especially for applications handling sensitive data. Encryption should be used for data at rest and in transit. Secure authentication methods, such as multifactor authentication, help protect user accounts. Access controls ensure that only authorized users can access specific data. Regular security updates and patches are necessary to protect against vulnerabilities.

CAREERS IN IS

Data Quality Analyst

A data quality analyst is a professional who is responsible for the data cleanliness and security within an organization. Following are some key responsibilities of this role:

- Data cleaning: Resolve issues such as incorrect formatting, duplicate entries, missing values, and other outliers.
- Data validation: Ensure accuracy and compliance through comparing data with predefined rules and

standards.
- Data governance: Enforce quality policies to maintain the integrity of the data.
- Data standardization: Maintain consistent formatting throughout data sources.
- Data security: Implement security measures that protect data.

Privacy and Data Protection

Protecting user privacy involves adhering to data protection regulations such as the General Data Protection Regulation (GDPR), HIPAA, and the California Consumer Privacy Act (CCPA). Users should be informed about what data are being collected, how the data will be used, and who the data will be shared with. Providing options for users to control their data, such as opting out of data collection and deleting their data, is essential for building trust.

Design Principles for Mobile Applications and Database Management Systems

Successful apps are well designed and allow the user to easily navigate the interface. Several principles can ensure an effective mobile application design:

- Simplicity and clarity: Keep the user interface straightforward to reduce the risk of user input errors. This includes reducing clutter on screens and only displaying essential information to reduce cognitive load for users.
- Consistency and reliability: Maintain a consistent style (interaction behaviors, colors, fonts, layout patterns) across the application, and ensure it functions in accordance with its designed specifications, with no or minimal failures during the specified time of its use.
- Accessibility and usability: Ensure accessibility for those with disabilities, through features such as adjustable text sizes, appropriate color contrast, and functions like text-to-speech. Make sure users have adequate time to interact with the system so it is easily usable. This includes functions like response time, the ability to provide feedback, and verification of option selection or payment.

A mobile app DBMS is essential to ensure smooth app functionality. Some key principles for an efficient DBMS include the following:

- Modularity: Break the system into manageable parts, such as separate modules for user authentication, data collection, and data retrieval.
- Flexibility: Design the database to handle changes in data requirements or formats without needing extensive rework. This is especially important for large, unstructured data from apps such as real-time messaging or social media platforms.
- Scalability: Ensure the system can handle increasing amounts of data and users, which is especially important for growing mobile applications.
- Security: Implement robust security measures, such as encryption and access controls, to protect data during transmission and storage.

Cloud-Based Databases

Cloud-based databases offer several advantages, including scalability, flexibility, accessibility, and cost efficiency. They can easily scale up or down based on demand, support various data models, and provide pay-as-you-go pricing models that reduce up-front costs. Major cloud-based database services include AWS with Amazon RDS and Amazon DynamoDB, Microsoft Azure with Azure SQL Database, and Google Cloud with Cloud SQL. Cloud-based databases are widely adopted across industries due to their ability to handle large data volumes, provide robust disaster recovery options, and support real-time analytics. They are particularly useful for industries with fluctuating data needs, such as e-commerce during holiday seasons or health care during public health crises.

GLOBAL CONNECTIONS

Netflix Database

Think about Netflix, a company that streams movies and TV shows to millions of people across the world. Behind the scenes, Netflix relies on a powerful database system to keep everything running smoothly. The company experienced rapid growth that made it difficult to keep up with customer demand. This growth led to a database corruption in 2008, which made the company realize that they had to make the switch to a cloud database.[4]

Netflix completed its cloud migration in 2016.[5] By using cloud-based databases, Netflix became able to handle a huge number of users at the same time, making sure videos loaded quickly and without interruptions. It also allowed Netflix to personalize what recommendations customers saw, so every viewer received a unique experience.

Considerations for Cloud-Based Databases and Their Architecture

Cloud-based databases are hosted on third-party servers, providing scalable and flexible data storage solutions. This means businesses don’t have to maintain physical servers and infrastructure, freeing them to focus on development and other core activities. Examples include AWS with Amazon RDS and DynamoDB, GCP with Cloud SQL and Cloud Firestore, and Microsoft Azure with Azure SQL Database and Azure Cosmos DB.

Third-party providers manage these cloud-based databases. They handle the infrastructure, including database farms and storage. This ensures high availability, data redundancy, and automatic backups, which reduces the operational burden on businesses. Services like Amazon RDS, Google Cloud SQL, and Azure SQL Database offer managed database services, taking care of patching, backups, and scaling.

Cloud applications benefit significantly from the scalability and flexibility of cloud databases. These databases allow applications to handle increased loads without performance issues, which is especially important for mobile applications that experience varying levels of user activity.

- Bandwidth: Cloud databases need to handle high data transfer rates efficiently. Adequate bandwidth ensures that data can be transmitted quickly between the cloud database and the mobile application, providing a smooth user experience.
- Redundancies: Redundancy is built into cloud architectures to ensure data availability. Cloud providers use techniques such as data replication across multiple geographic locations to protect against data loss and ensure that services remain available even in the event of hardware failures.

Pros and Cons of Cloud-Based Databases

Most organizations choose cloud-based databases because they make storing and managing data easier and more flexible. Some of their benefits include being able to scale as needed and access data from anywhere, but there are also drawbacks, like security risks and potential cost issues. Organizations will need to weigh the pros and cons to determine if they’re the right fit for the organization’s needs. Some pros of cloud-based databases are as follows:

- Scalability: Cloud-based databases can grow or shrink with needs, which can easily accommodae fluctuating workloads.
- Cost-effectiveness: Customers only pay for what they use, so there’s no need for costly investments in hardware.

4 Yury Izrailevsky, Stevan Vlaovic, and Ruslan Meshenberg, “Completing the Netflix Cloud Migration,” Netflix, February 11, 2016, https://about.netflix.com/en/news/completing-the-netflix-cloud-migration
5 Yury Izrailevsky, Stevan Vlaovic, and Ruslan Meshenberg, “Completing the Netflix Cloud Migration,” Netflix, February 11, 2016, https://about.netflix.com/en/news/completing-the-netflix-cloud-migration

- Easy access: Customers can access their data from anywhere with an internet connection.
- Automatic updates: The cloud provider takes care of software updates and security patches, so organizations don't have to worry about maintaining the system.
- Disaster recovery: Most cloud services have built-in backups and recovery options to protect data from loss or outages.

Some cons of cloud-based databases are as follows:

- Internet reliance: If the internet goes down or is slow, it can disrupt access to the database.
- Security risks: Storing data in the cloud can raise concerns about privacy.
- Costs: While they can be a cost-effective option for small workloads, unexpected usage can drive up costs quickly.
- Less control: Organizations may have limited control over the database compared to hosting on their own infrastructure.
- Vendor lock-in: Switching to a different cloud provider can be complicated and expensive.

FUTURE TECHNOLOGY

Smarter Streaming with Artificial Intelligence

Netflix uses a mix of relational and NoSQL databases like Apache Cassandra, MySQL, and DynamoDB to manage all the data it needs for streaming. These databases work together to store and organize user information, the massive content library, and details like what shows people watch and how long they watch them.

But Netflix takes it a step further by using AI to personalize the experience. The AI systems analyze the data from these databases to figure out what users might want to watch next. For example, Cassandra handles huge amounts of real-time data from around the world, MySQL keeps track of account details, and DynamoDB supports the AI recommendations that pop up while browsing for something new.

By combining its databases with AI, Netflix makes sure users get spot-on recommendations, smooth video quality, and a seamless experience no matter where they are or what device they're using.

Key Terms

access control security-driven restriction of access to ensure that only authenticated users are able to interact with specific resources

ACID (atomicity, consistency, isolation, and durability) characteristics that ensure transactions are fully completed or not executed (atomicity), the database remains accurate and follows its rules (consistency), transactions do not interfere with each other (isolation), and a transaction stays saved even if the system crashes (durability)

B-tree index most common type of index; maintains a balanced tree structure, providing efficient insertion, deletion, and lookup operations

back end part of a software application that handles data, logic, and operations, supporting what users interact with on the front end

bitmap index type of index that uses 0s and 1s to show where a value is in a database

check constraint rule that specifies the value that can be entered into a column

conceptual design creation of a simple model of data for database design, focusing on what is needed and how it is connected

data cleanliness accuracy and consistency of data and the lack of duplicated or missing information

data consistency data remain consistent and accurate across the database

data independence data can be restructured without affecting the programs that use it

data lake type of database that stores large amounts of raw data in their original format until the data are needed

data life cycle stages that data undergo from creation to deletion, ensuring data remain accurate, accessible, and valuable throughout their life cycle

data redundancy duplication of data

data retrieval process of obtaining specific information from a database or storage system

data warehouse type of database that integrates data from various sources and stores them in a combined manner

database access tool provides graphical user interfaces (GUIs) to facilitate database interaction without writing extensive code

database management system (DBMS) software system that manages, stores, and process data, ensuring it is organized, accessible, and secure

database schema structure of tables, including columns and data types

denormalization addition of redundant data for the purpose of making things run faster and meeting specific requirements

foreign key column or set of columns in one table that establishes a relationship with the primary key in another table

front end part of a software application that users interact with, including the design and user interface

functional dependency how one piece of data relates to another within a table

hash index type of index that uses a hash function to map data to a fixed-size table

indexing technique used to improve the speed of data retrieval operations in a database

integration test test to check the interaction between modules

logical design detailed database model that defines tables, columns, primary keys, and foreign keys

normalization technique in the design process where data are organized and stored only once, to eliminate the duplication of data

NoSQL database (Not Only SQL) database that does not use the traditional table structure of SQL databases

NoSQL database management system type of database that provides a mechanism for storing and retrieving data that is not based on the traditional relational database model

object-oriented database management system (OODBMS) database management system that stores data in the form of objects, similar to the way data are represented in object-oriented programming

orphaned record record that references another record that no longer exists

physical design creation of a physical structure from a logical design via actual implementation in the database

primary key unique identifier for each data entry in a database table

referential constraint maintains relationship between tables, making sure that a foreign key in one table matches a primary key in another table

relational database stores data in tables with rows and columns, making it ideal for structured data

relational database management system (RDBMS) database management system that stores and organizes data in a structured way using tables

requirements analysis studying how a business operates to determine what data should be stored and how the data should be used

semistructured data data that have some organization but do not fit neatly into tables

structured data data that are highly organized and easily searchable

Structured Query Language (SQL) standard language used to query and manage data in relational databases

system test test to evaluate the overall functionality

unit test test to verify individual functions

unstructured data data that lack predefined structure and require advanced techniques for analysis

user acceptance testing test to ensure the system meets the needs of end users

Summary

3.1 Data Types, Database Management Systems, and Tools for Managing Data

- A database management system (DBMS) is a software system that manages, stores, and processes data, ensuring data are organized, accessible, and secure.
- Data can be categorized into structured, semistructured, and unstructured types, requiring different tools and techniques to collect and analyze. Data come in two main types: line of business data and customer behavior data.
- Managing data effectively is essential for organizations to ensure data integrity, accessibility, and security. A database system provides a structured environment to store, retrieve, and manipulate data efficiently.
- Building a database involves two steps—design and implementation—to ensure that a structure can efficiently store and manage data. Types of databases include relational, NoSQL, data warehouses, and data lakes.
- Understanding the types of data storage, indexing, and data retrieval techniques is fundamental to understanding database concepts.
- Database design is the process of organizing data according to a database model, developing a design through conceptual, logical, and physical stages. Strong design involves understanding the data needs of an organization and structuring the data to minimize redundancy and maximize performance, and meeting requirements for functional dependencies and normalization.
- Building a database involves gathering, organizing, curating, and processing data, as well as allowing for security and access controls.
- Types of database management systems include relational, object-oriented, and NoSQL.

3.2 Practical Applications of Database Design and Management

- Database design and management are important for businesses because they help store, organize, and retrieve data efficiently.
- A good database design ensures data are accurate, secure, and easy to access.
- In e-commerce, databases help manage product inventory, track customer orders, and analyze sales. In healthcare, they manage electronic health records (EHRs).

- Logical design involves creating a blueprint of the database that outlines the structure without considering how it will be physically implemented.
- Physical design focuses on how the database will be built on a specific DBMS.
- A systems design process outlines the steps involved in creating a system, ensuring a systematic approach to design and leading to successful project outcomes.
- Testing, documentation, and maintenance ensure that the DBMS meets all requirements and performs as expected under various conditions.
- Applications of DBMSs can be found in various industries, such as health care, finance, education, and manufacturing.

3.3 Mobile Database Development and Cloud Database Management Systems

- Mobile development and cloud databases are closely linked as more businesses look for scalable and efficient ways to support their apps.
- Mobile app development is closely tied to database design because apps rely on databases to store, manage, and retrieve data. Whether it's user profiles, messages, or product details, the database handles this information.
- In mobile app development, using cloud databases lets developers focus on user experience and app features without worrying about data storage and management.
- Mobile applications need to handle various forms of data input efficiently and accurately, ensuring that the collected information is stored securely and is easy to retrieve.
- Cloud applications benefit significantly from the scalability and flexibility of cloud databases.
- Cloud databases need to handle high data transfer rates efficiently.
- Cloud providers use techniques such as data replication across multiple geographic locations to protect against data loss and ensure that services remain available even in the event of hardware failure.

Review Questions

1. Which of the following best describes the two main types of data and their focus areas in business operations?
   a. Line of business data focus on customer interactions and feedback, while customer behavior data include daily operations and financial records.
   b. Line of business data involve daily operations like financial records and supply chain details, while customer behavior data focuses on customers' interactions with a company's offerings, such as purchase history and social media interactions.
   c. Line of business data include social media interactions and purchase history, while customer behavior data involve inventory processes and supply chain details.
   d. Both line of business data and customer behavior data focus primarily on the financial records and day-to-day operations of a business.

2. The type of data that includes photos and scanned documents is called ________.
   a. text data
   b. voice data
   c. image data
   d. video data

3. A tool or technique *not* used for managing data in a database system is a(n) ________.
   a. Structured Query Language (SQL)
   b. database management system like MySQL
   c. image editing software like Adobe Photoshop
   d. database access tools like phpMyAdmin

4. The type of database designed to handle a wide variety of data types and structures, providing flexibility for applications like real-time web applications, is a(n) ________.
    a. NoSQL database
    b. relational database
    c. data warehouse
    d. data lake

5. An example of a primary data source are ________.
    a. data from existing databases
    b. articles and books
    c. direct observations
    d. reports from other researchers

6. Database design and management are crucial for businesses because they ________.
    a. help in storing, organizing, and retrieving data efficiently
    b. ensure data are accurate, secure, and easy to access
    c. support various enterprise systems like customer relationship management, financial systems, and health-care information systems
    d. all of the above

7. What is the main benefit of electronic health record systems in health care?
    a. storing patient information, medical histories, and treatment plans
    b. helping with marketing strategies
    c. managing product inventory
    d. tracking financial transactions

8. What is the primary purpose of requirement analysis in the design of a library management system?
    a. determining the feasibility of the project
    b. gathering and analyzing user needs
    c. creating data models and defining system architecture
    d. conducting testing and ensuring system functionality

9. Why are cloud databases important for mobile app development?
    a. They offer lower maintenance costs and real-time data access.
    b. They increase the complexity of app development.
    c. They require local servers for data storage.
    d. They eliminate the need for user experience design.

10. How do cloud-based databases benefit mobile applications?
    a. They reduce the need for user authentication.
    b. They eliminate the need for data encryption.
    c. They provide scalable and flexible data storage solutions.
    d. They require businesses to maintain physical servers.

Check Your Understanding Questions

1. What is indexing in the context of databases, and how does it improve data retrieval operations?

2. What is the purpose of referential constraints in database design, and how do they ensure data integrity?

3. What are the primary advantages of using NoSQL databases over traditional relational databases?

4. How do document-oriented databases handle data, and what are their typical use cases?

5. How do well-designed databases improve operations in health-care systems?

6. Explain the role of databases in e-commerce and how they enhance customer satisfaction.
7. What are the key components and functionalities that a library management system must handle?
8. What steps are involved in the feasibility study for designing a library management system, and why are they important?
9. How do cloud databases support the scalability and efficiency needs of mobile applications?
10. What are some key design principles to consider when integrating mobile applications with databases?

Application Questions

1. You are a database architect for a company that develops different types of applications, including an ecommerce platform, a real-time analytics tool, and a computer-aided design system. Your job is to choose the right database management system for each application. You have these options:

   - relational database management system (RDBMS)
   - object-oriented database management system (OODBMS)
   - NoSQL database

   Based on this scenario, answer the following questions:

   a. Which DBMS should be chosen for the e-commerce platform and why?
   b. Which database management system would be most appropriate for the real-time analytics tool and why?
   c. Which database management system should be selected for the computer-aided design system and why?

2. Given the importance of security in database design, particularly in systems handling sensitive data such as a library management system, outline the security measures you would implement to protect the data.

4 Systems Analysis, Design, and Development

Figure 4.1 Something as simple as picking up medicine from a pharmacy entails a complex set of actions that require careful design by systems analysts who work in information systems development. (credit: modification of work "Controversy Surrounds Prescription Drug Monitoring Program" by Jiselle Macalaguin, KOMUnews/Flickr, CC BY 2.0)

Chapter Outline

Introduction

When you step into a pharmacy to pick up a prescription, the simple act is one point in a complex set of systems and actions. The system checks your prescription and ensures that it is reliable and valid. It then allows the pharmacist to dispense the requisite prescription and provides the notes to be printed for the patient and/or caregiver to ensure that the right dosage is taken for the time frame prescribed by the physician. In some cases, the information system also checks for allergies or other medications that may result in an adverse reaction for the patient. As a safety measure, this information, if available, is also provided in the notes provided with the prescription. This is just one example of how your daily life intersects with the design and development of information systems.

4.1 Systems Analysis and Design for Application Development

Learning Objectives

By the end of this section, you will be able to:

- Describe the concept of systems analysis and design
- Identify methodologies and tools used in systems analysis and design
- Explain, compare, and contrast the software development life cycle (SDLC) and Agile software development
- Describe the roles and responsibilities of analysis and design teams

The evolution of software projects from conception to implementation relies on tools that guide the design and ensure alignment with user needs and organizational goals. Throughout system development , the contributions of various teams and the methodologies they adopt play a pivotal role in shaping outcomes, with each phase offering unique challenges and opportunities for collaboration. To understand the concept of systems analysis and the design methodologies used for application development, you must also become familiar with the software development life cycle (SDLC) and Agile software development, as well as the roles and responsibilities of the analysis and design teams.

Systems Analysis and Design

The stepwise process for evaluating and developing information systems by understanding the needs of the business to improve or develop effective and efficient functioning solutions to technical challenges is called systems analysis and design. You may recall from Chapter 1 Fundamentals of Information Systems that information systems combine the people, processes, data, hardware, and software needed to collect, store, process, analyze, and distribute data. Examples of information systems include order processing, inventory control, human resource management, and sales management systems. Consider one information system you have probably encountered already: a prescription order process linking a prescribing doctor to a pharmacy. In Figure 4.2, you can view the workflow of a prescription request traveling from the prescriber through an electronic health record system toward the pharmacy staff and its system. In this scenario, there is an intermediate interaction with an e-prescription vendor's system that is designed to translate and process that request so the receiving pharmacy staff can satisfy the doctor's request for a patient's medication.

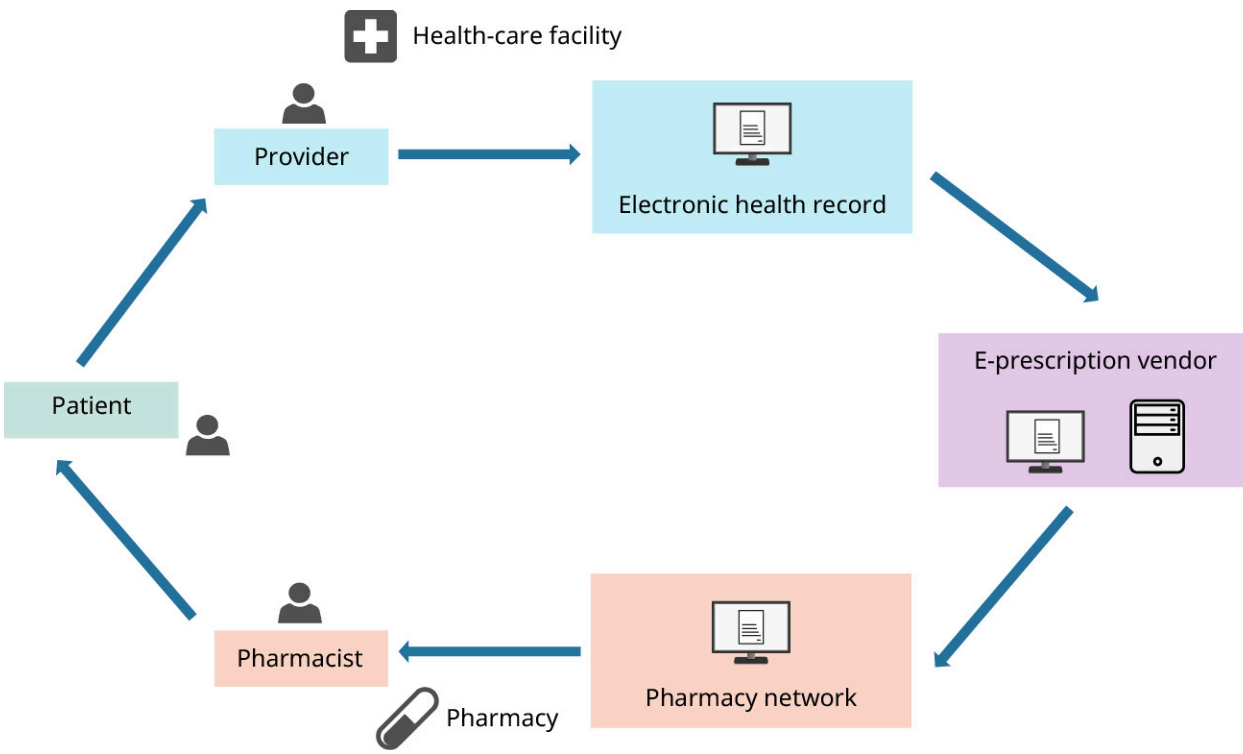


Figure 4.2 The prescription order process involves several systematic steps beginning with the prescriber sending a patient's medicine order to an electronic health record database, which forwards it to a vendor, who then routes the order to a pharmacy's internal system and staff, who finally provide the medicine to the customer. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit capsule: modification of work "Pill – The Noun Project" by Noelia Bravo/Wikimedia Commons, CC0 1.0; credit hospital sign: modification of work "Ic local hospital" by Google Inc./Wikimedia Commons, CC BY 4.0)

Who would think there were so many steps involved with picking up a prescription from a local pharmacy? Starting at the doctor's office, the physician submits a prescription order through an online ordering system to the patient's preferred pharmacy. The pharmacy, upon receipt of the prescription order, processes the prescription accordingly by validating patient information such as insurance, reviewing the aspects of the order, preparing the medication, and conducting a final review before providing the patient with the medication and instructions for use. There are many systems at work in this scenario—systems that connect users (i.e., medical and pharmacy staff), hardware (i.e., computer, keyboard, central processing unit or CPU, and wireless routers), software (electronic health record or EHR, ePrescribe software, and pharmacy benefit management tools), and other devices, working together to provide services.

Businesses initiate systems analysis and design to assess workflows, identify improvements, and create efficient systems. Some companies have formal processes with a task force led by a senior manager, while others approach systems analysis and design on an ad hoc basis. Organizations may prioritize projects using various criteria, tools, techniques, and input from multiple departments in order to align projects with business objectives. These initiatives often lead to systems analysis that can inform future design changes.

LINK TO LEARNING

The International Institute for Business Analysis (IIBA) is an internationally recognized organization that works on developing industry standard business analysis practices and resources. The IIBA, which has global reach, also considers a business's mission, values, and goals to implement a systems thinking approach. Learn more about the IIBA's practice of business analysis (https://openstax.org/r/109IIBABusinAny) from IIBA's In the News section of their website.

Benefits of Systems Analysis and Design

Systems analysis and design offers several benefits to an organization, with the primary advantage being the identification of operational efficiencies through improvements to existing systems. This process also allows organizations to align their information systems with their strategic objectives, identify the risk of potential threats to processes early, minimize resources and costs, and improve the overall quality, efficiency, productivity, and usability of their systems.

A **systems analyst** is a professional whose primary function is to utilize the systems analysis and design process to support information systems and to solve challenges associated with or posed by using the information systems. Systems analysts are often regarded as a conduit between information technology departments and business areas of the organization as they work to understand how an information system is used to support business functions and identify the challenges that persist and areas that need improvement. Although systems analysts are increasingly serving in information technology departments, they may also work in different areas of the business, such as operations, finance, marketing, sales, or human resources.

Systems Analysis

The process called **systems analysis** identifies the opportunities that can be discovered by examining business problems and develops possible solutions an organization may implement to address these problems. Systems analysis generally involves the following three activities: understanding the current business problem; determining the system requirements, constraints, and information needs; and generating a systems analysis report (Figure 4.3).

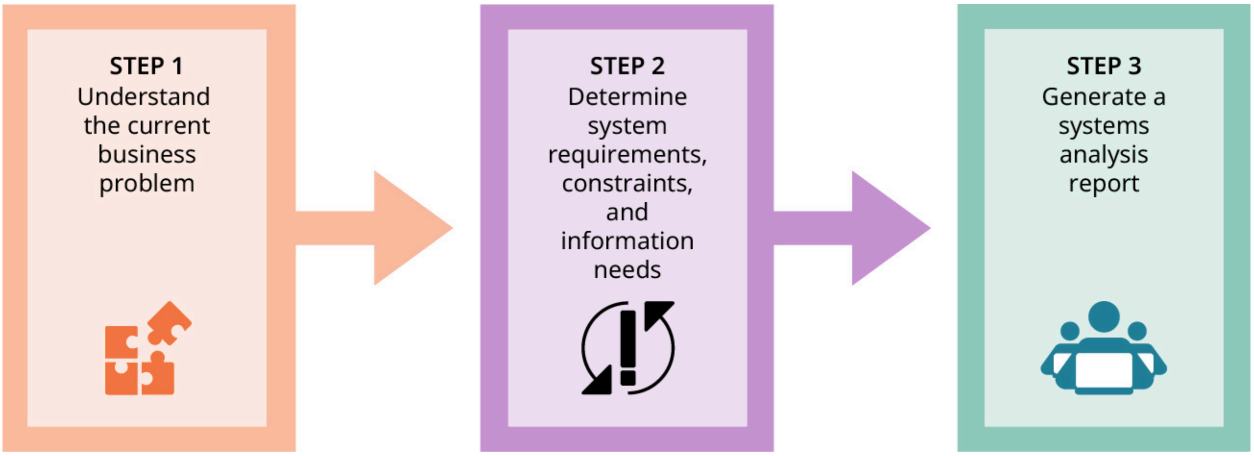


Figure 4.3 Understanding the current business problem; determining system requirements, constraints, and information needs; and generating a systems analysis report are the three basic components of systems analysis. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit left: modification of work "Noun Planning 1325509" by Arafat Uddin/Wikimedia Commons, CC BY 4.0; credit middle: modification of work "Noun Project problems icon 2417098" by Template, TH/Wikimedia Commons, CC BY 3.0; credit right: modification of work "Noun project - Meeting with laptops" by Slava Strizh/Wikimedia Commons, CC BY 3.0)

Understanding the Current Business Problem

In defining the business problem, detailed information about the information system is gathered and analyzed using a variety of tools and techniques. To understand the business problem, the systems analyst first identifies stakeholders. A **stakeholder** is an individual or group who has a vested interest in or concern about a business decision. They may be internal or external to an organization and may include the community, government entities, employees, customers, investors, suppliers, or trade unions and associations. After identifying the stakeholders, the systems analyst begins the task of gathering information about the system to gain a better understanding of its functionalities and any challenges it currently faces. This information may include the purpose of the system, inputs and outputs, functional capabilities, number of users and levels of access, ease of use, accessibility, and challenges associated with its use.

Common methods used to gather this information or data include:

- System documentation review: The **system documentation** describes the system and its parts. It is used to understand how the system functions as well as serving as reference information. It may include requirements documentation, user guides, source code, architecture and design descriptions, and frequently asked questions (FAQs). By examining system documentation, the analyst may uncover how the system was originally designed to perform and changes made to the system since its initial use within the organization. The analyst may find that existing documentation may not be current, accurate, and/or complete. In that case, the analyst can work to revise and update the documentation for currency, accuracy, and completeness. Information-gathering may also involve examining policy documents and regulatory rules shaping the needs of the system.
- Surveys: A survey is a common form of information gathering. It allows larger groups of users to respond to an inquiry about a system so they can provide insight into its use. Surveys are usually affordable to administer, take minimal time, and can involve a variety of stakeholders across the organization.
- Interviews: The systems analyst may conduct interviews of different systems users and roles. To prepare for these interviews, the analyst will identify the objectives for the interview, generate and administer interview questions, document the results, and evaluate interview responses. Interviews may be structured (i.e., use the same interview questions and methods) or unstructured (i.e., involve no set format or predetermined questions). Interviews may take longer than other methods of information gathering but are useful in gaining insights that may not present themselves in surveys.
- Observations: Making observations about an information system generally involves noting how users perform their functions through and in relation to the system and, in turn, how the system responds. Observations may be passive (e.g., watching users perform actions without interference or influence) or

active (e.g., engaging with users and asking questions about the activities they perform). Web analytics or metrics may be used as a gauge of observations made. Inputs and outputs of the system are observed and then documented for further review and analysis.
- Data analysis: Once the system documentation is collected, it is systematically reviewed, cleansed, sorted, and condensed so that conclusions and insights can be drawn to help solve business problems. Generally utilizing qualitative and/or quantitative/statistical analysis techniques, data analysis can be an iterative process where the team may need to refine the data gathering process to gain a further understanding of the data presented.

Determining System Requirements, Constraints, and Information Needs

System requirements are the capabilities stakeholders request to make a functioning system that supports their business needs. They can be categorized as functional, nonfunctional, business, technical, legal/regulatory, and/or performance related. Generally, the systems analyst will collaborate with stakeholders to gather these requirements. Once collected and defined, requirements are then placed in categories and prioritized based on criteria important to the business. As you will learn in 4.3 Technical Design Methodologies and Practical Applications, systems analysts may go further and develop user interface designs that give a representation of how system requirements interact with the data rules and roles and even the constraints of the system functionality.

Access to system data about usage and functionality of the system is a key component to the user requirements. Reporting functionality that provides usage data at both the macro and micro levels can be helpful to assess both the system and the users of the system. One example of how system data serve as a key component of user requirements can be found in customer service call histories at data centers. Data about the details of a call (i.e., length, representative, day/time, reason for calling, resolution status) are usable for a variety of business purposes, including training, service improvements, and employee recognition. For example, the day and time associated with a call can point to a number of issues such as bandwidth availability or system processing issues, and this information can lead to changes in end-user training, needed system improvements, or identification of a group-specific issue. These system/user requirements and all supporting information are then reviewed, evaluated, and finalized with input from stakeholder users.

ETHICS IN IS

Values-Based Engineering

Today, algorithms and artificial intelligence are driving the techniques used for systems analysis, design, and development. This can lead to ethical concerns, eroding user trust. For example, a 2023 study revealed that Google’s job search tools returned more higher-paying positions to men rather than job seekers of other gender identities. In addition, job applicant tracking systems are often found to favor words in résumés more closely associated with men.[1] These systems have also placed nonnative speakers at a lower rank because of inherent bias from AI training on only one specific language.

The process of values-based engineering (VbE) helps to address these challenges within the approaches to analysis, design, and development. This is accomplished by defining, prioritizing, addressing, and integrating values into the requirements process. VbE is applicable to both functional and nonfunctional requirements through tools, standards, and best practice guidelines.

Generating a Systems Analysis Report

The systems analyst typically provides interim feedback to stakeholders throughout the process, and the final

1 IBM Data and AI Team, “Shedding Light on AI Bias with Real World Examples,” IBM, October 16, 2023, https://www.ibm.com/think/topics/shedding-light-on-ai-bias-with-real-world-examples

step involves generating a systems analysis report. This report is likely to include recommended solutions to address or resolve the information system problem, and these solutions may take the form of changes in business processes, including systems improvements, elimination, or changes.

LINK TO LEARNING

A systems analysis report often takes the form of a feasibility study. Review this example of a feasibility study template (https://openstax.org/r/109Feasibility) that might be shared with stakeholders. It also features a survey asking shareholders to assess the viability of a proposed project.

Systems Design

A **systems design** is an organizational approach that aims to improve an existing system or to develop a newer one. This process involves doing the technical work of defining the data, interfaces, and overall architecture of a system based on user requirements and determining how these elements communicate with each other to produce a reliable, robust, and well-documented system.

Before designs are made, the organization needs to decide whether to develop the new system or improve the existing one by outsourcing, buying off-the-shelf, or using in-house development. In-house systems development typically leads to systems design that generally includes data design, interface design, and process design, which could be performed in any order.

- Data design: The activity of **data design** is when data and the actionable components resulting from the systems analysis process are translated from their raw formats and combined into understandable formats such as textual data (e.g., TXT), tabular data (e.g., spreadsheets), or images (e.g., PNG or JPEG) is called data design. At this stage, you can envision how the data and actionable components blend and create patterns, correlations, and trends into interactive systems. This is where works is done to reduce the complexity and improve the understanding of the information presented into usable formats.
- Interface design: The process of **interface design** refers to designing the visual layout and functional elements of a product or system, and it involves using an understanding of people and processes to drive the final design outcomes.
- Process design: The effort to further understand a business's processes and how to improve them is called **process design**. It can support decision-making on new business ventures, expansions, and other business functions by breaking down the product into parts and identifying areas of operational efficiencies.

Tools in Systems Analysis and Design

Several tools play a part in systems analysis and design. Several of the most common are data dictionaries, simulations, pseudocode, structured English, and unified modeling language. A data dictionary is a database that houses the details of system data, its properties, entity relationships, and any reference documentation. A simulation is a model that mimics the operation of an improved or proposed system. The plain English steps for an algorithm or other system that cannot be used in a compiler are called pseudocode, and structured English is a sequence of decision rules that uses the English language with the syntax of structured programming and the convention of IF-THEN-ELSE. Another tool that can be used to lay out the blueprint at various levels in a system is a simplified modeling language called unified modeling language (UML).

These tools are useful in creating diagrams of various system functions and relationships to gain deeper understanding during systems analysis. A **data flow diagram (DFD)** is a graphical representation of the information flow of a process or system. Another helpful diagram type is a UML diagram, which can show lower-level user interactions with the system as well as a high-level overviews of several activities working together in the system. A **UML diagram** represents a broad category of tools that are commonly used in systems analysis and design. These diagrams outline how a system will function from a user's perspective, and they feature use cases, sequence diagrams, activity diagrams, state diagrams, and class diagrams.

- Use cases: A use case describes those individuals who will use and interact with the system. In the scenario from Figure 4.2 of getting a prescription filled, the use case would map out how each user (the patient, the doctor, the pharmacy, the insurance company) interacts in the system. UML diagrams can also be accompanied by a written use case, which includes details about the interaction of the users with the system rather than simply a visual representation.
- Sequence diagrams: A sequence diagram is used to illustrate a particular part of the system, not the entire system. They are specifically used when parts of the system must work in a certain order (Figure 4.4). Returning to the sample scenario, for the patient to eventually pick up their prescription, a doctor must first write that prescription and send that information to the pharmacy. Those system actions have to occur in that order. A patient cannot go to the pharmacy and get their medication prior to the prescription order coming from the doctor. The sequence diagram provides a general overview of the sequential process in the system.
- Activity diagrams: An activity diagram is used to represent how several use cases are coordinated together in a system. They are used to visualize more complex activities in the overall system (Figure 4.5).
- State diagrams: A state diagram is similar to an activity diagram; however, it is used to visualize behavior in a system based on the state the system is in. For example, the prescription ordering system might behave differently if the medication ordered by the doctor belongs to a certain class of controlled substances. The state diagram would then include the additional reporting procedures or other related activities that are required before the medication can be released to the patient (Figure 4.6).
- Class diagrams: A class diagram provides the building blocks for the system. These diagrams show each class and its associated attributes. The diagrams also show the relationship between classes in the system. For example, in the prescription ordering scenario, the patient is a class with attributes such as name, address, and insurance provider. The pharmacy itself is also a class, with attributes that might include location and medications stocked.

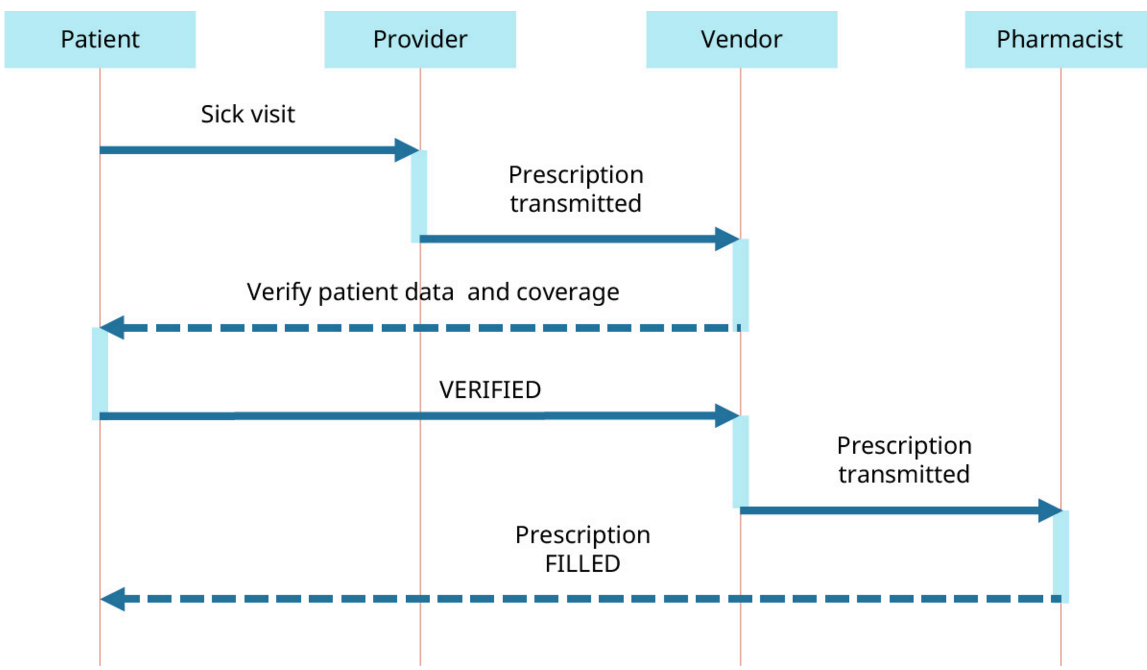


Figure 4.4 To easily understand how part of a system works, a sequence diagram can be helpful. This simplified sequence diagram shows how a patient can get a prescription. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

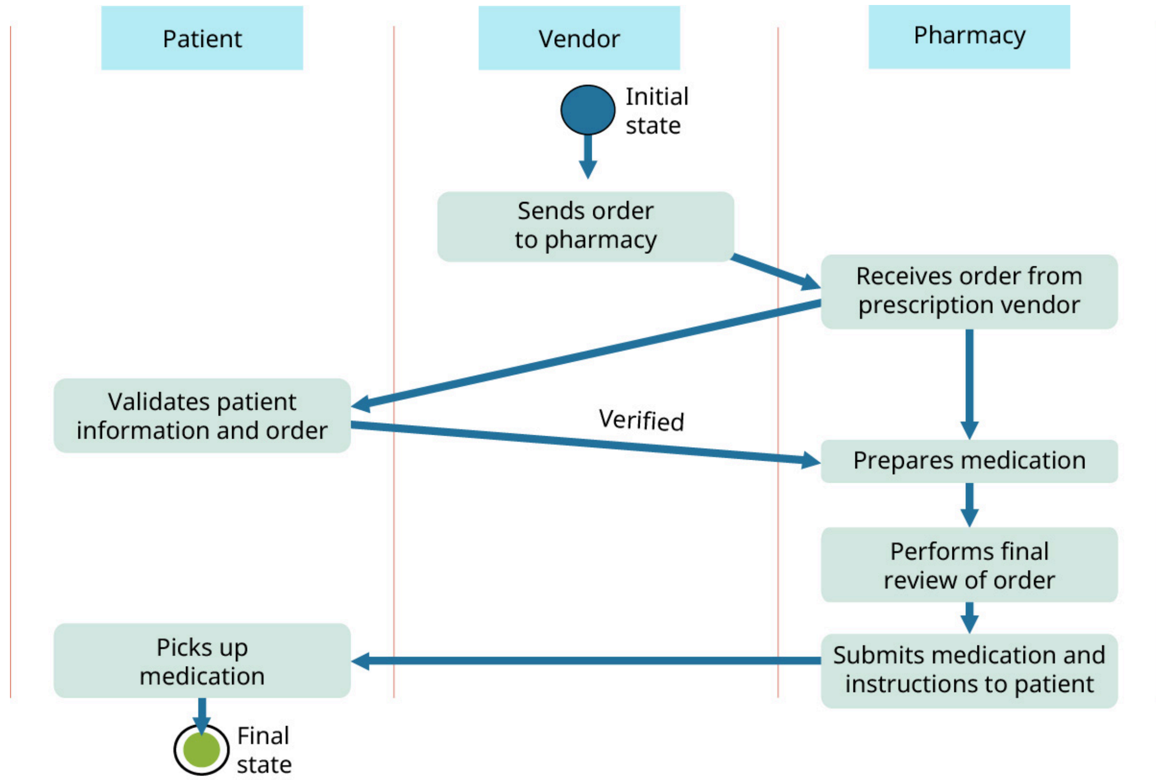


Figure 4.5 An activity diagram illustrates complex activities in the system for better understanding. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

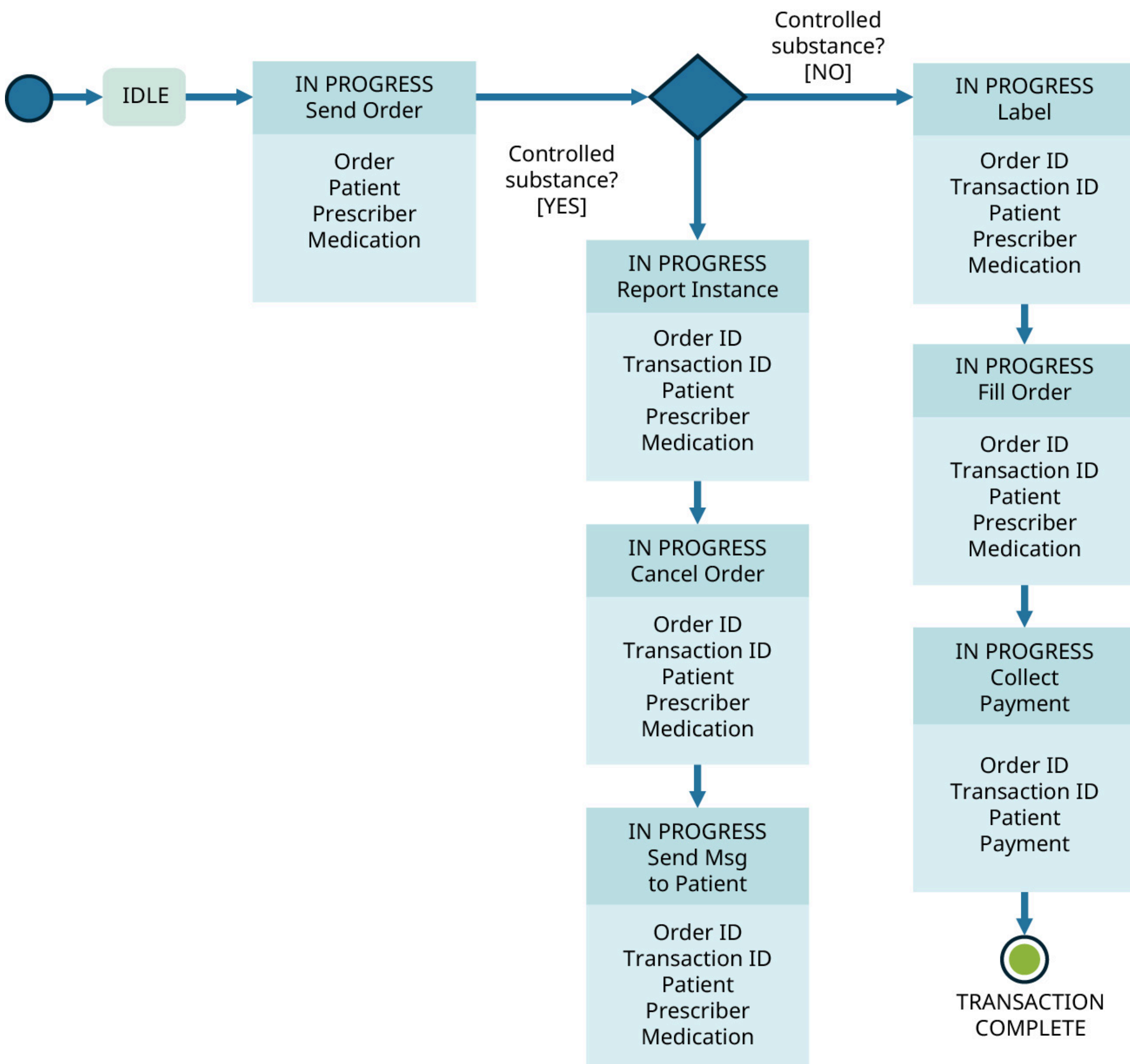


Figure 4.6 A state diagram illustrates different behaviors of the system dependent on the state the system is in. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Software Development Life Cycle and Agile Software Development

The **software development life cycle (SDLC)** is a framework that defines the stages of software development, from its inception to its retirement, providing a blueprint of the tasks to be completed for each stage of the cycle (Figure 4.7). Following the recommended SDLC process will lead to a quality product that was created in a systematic and disciplined fashion. The six stages of the SDLC process are analysis, design, development, testing, deployment, and maintenance.

1. Analysis: In the analysis stage, time is spent with the customer to collect relevant information needed to develop the product, keeping the potential design and code in mind. Business analysts and project managers are generally involved in this activity, especially when meetings with the customer will generate user requirements or aspects of a solution, stated by stakeholders, that are needed to support specific needs and expectations of a business process or product. Systems analysts make sure to discuss each aspect of the requirements with the stakeholder to remove ambiguity and to increase clarity and understanding.
2. Design: During the design stage, the user requirements are used as inputs for the design approach. The

developer reviews this information to assess the prepared software against the requirements of the end users. Design specifications are created, reviewed by stakeholders, and approved for development.

3. Development: The development stage is sometimes called the implementation or coding phase as this is where these activities begin. The design is translated into source code or computer-legible language—meaning the developer builds the system in a coded language using coding guidelines and programming tools. This stage is the longest in the SDLC life cycle.
4. Testing: Once the development stage is complete, testing of the design is initiated to validate the system functions against the requirements and to identify any bugs or defects within the coding. Often, this occurs within a separate testing area, away from the development and production environment for the product. Developers review the feedback and fix identified problems, updating the components for retesting.
5. Deployment: During the deployment stage, the product is released for customer or stakeholder use. Some testing is also completed in the production environment, which now houses the new product and the approved, validated coding. Documentation on product use generally accompanies this release.
6. Maintenance: The maintenance stage occurs after the product is deployed and is functioning within the production environment, when intermittent patches and fixes may be needed to improve the usability of the product. Additionally, any proposed enhancements may occur during this maintenance period.

Figure 4.7 The SDLC is a cyclical framework that defines the stages of software development, from its inception to its retirement, providing a blueprint of the tasks to be completed for each stage of the cycle. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Agile Software Development

Organizations continue to identify efficiencies in the software development process and are increasingly using the Agile methodology. **Agile** is an overarching term describing the iterative and incremental delivery of quality products and value to stakeholders using team collaboration, flexibility, and continuous planning. **Agile software development** is an adaptive approach to software development that considers uncertainty in changing environments and allows "Agile" teams to respond to changes quickly by delivering smaller, consumable work packages. The need for a software development approach that allowed for this flexibility, value, and collaboration was identified by a group of like-minded individuals who created the Manifesto for Agile Software Development, which features four Agile Manifesto values (Figure 4.8).

The Agile Manifesto		
"We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:		
Individuals and interactions	*over*	processes and tools
Working software	*over*	comprehensive documentation
Customer collaboration	*over*	contract negotiation
Responding to change	*over*	following a plan
That is, while there is value in the items on the right, we value the items on the left more."		

Figure 4.8 The Manifesto for Agile Software Development was created by seventeen like-minded software developers whose combined thoughts and ideas led to the development of this adaptive approach to manage software development work. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

This approach emphasizes valuing certain aspects of software development over others:

- Individuals' interactions are valued over processes and tools. The Agile approach focuses on bringing the right stakeholders together to find a solution. Collaboration is at the forefront of the development process.
- Working software is valued over comprehensive documentation. Although documentation is needed, the end goal is a functioning system that meets the needs of the stakeholders with valued-added documentation components. The documentation required should not get in the way of providing a functional system.
- Customer collaboration is valued over contract negotiation. Often with negotiations, one party feels like the winner, while the other feels as if they lost. Agile software development utilizes collaboration throughout the process to build a teamwork mentality to create the most value for the stakeholders.
- Responding to change is valued over following a plan. Traditional development processes often follow a rigid timeline where changes typically result in additional costs and delays. The Agile approach incorporates changes into the planning process through evaluative feedback from stakeholders. This often means that the timeline and plan evolve, and the development of the system evolves.

Historically, software development has been performed using the SDLC. This approach is very systematic and is process oriented, moving from one stage to the next in the process. There are some parallels between the two methods, however. Both SDLC and Agile software development involve planning documentation, feedback, and testing of the system. With the Agile approach, however, there is much greater flexibility to incorporate changes and end-user feedback at all points in the development process. The SDLC approach can be used with any size project, whereas the Agile method is, at times, better suited for smaller-scale projects. With SDLC, no changes are typically made after the initial stages, and there is little interaction with the end user (customer). In contrast, end users are consulted at regular intervals in the Agile approach. Finally, with SDLC, the project moves through stages, whereas the Agile approach uses the term "phases" to better illustrate the fluid nature of the process as the development progresses.

Imagine scaling up a point-of-sale (POS) system to accommodate the needs of a new boutique, opening both an online storefront as well as a physical location. Fenner Street Boutique is set to open in the downtown area of a midsize community that has invested in attracting unique shops for residents and visitors. The boutique has a five-year goal to open a new location in a neighboring city with long-term plans for franchising. The POS system will be used for inventory control and managing both the on-site and online sales. The Agile approach would be particularly well-suited for such an application because there is uncertainty about the five-year goal and the inventory that will be sold online and in the store. The Agile approach is more suited to accommodate the uncertainty and will allow the business owner to incorporate needed adjustments as the business model develops after opening. The business owner will be involved in the development and share crucial information with the team about how the POS system will be used now and in the future. The process allows for the speed, flexibility, and creativity that is needed for growing business.

The main tenets of the Agile Manifesto hold value for applications beyond simply software development. The Agile framework has migrated to a wide variety of applications in business development, including marketing, finance, and human resources.

How Does Agile Development Work?

Although the Agile approach's process may seem unclear in its flexibility, there are central components of the development process that are key to success. Rather than stages or steps, the components can be best viewed as phases.

- A first step in the development process involves planning and preparation to bring together the right individuals to work on the team. This team might also include key stakeholders from the organization to ensure their input is at the forefront of the systems development, as illustrated in Figure 4.9.
- An assembled Agile team, consisting of a small group of individuals assigned to the same project or product, creates the plan for completing the identified requirements and a final product. The team identifies the features that will make up the final product and the order in which these features will be delivered. These features are referred to as the product backlog (or road map).
- After the product backlog is established, the work of developing the software begins.
- Regular meetings with the Agile team and the product owner are held to gauge the status of work in progress. User stories are the functional components of the work that are defined in conjunction with the product owner or stakeholder. Each of these stories is expected to add to the completed final product.

Figure 4.9 shows the continuous evaluative nature of the Agile approach. The system that is eventually launched is developed with stakeholder input, reevaluation, and adjusting as necessary to provide a solution to meet the needs of the product owner.

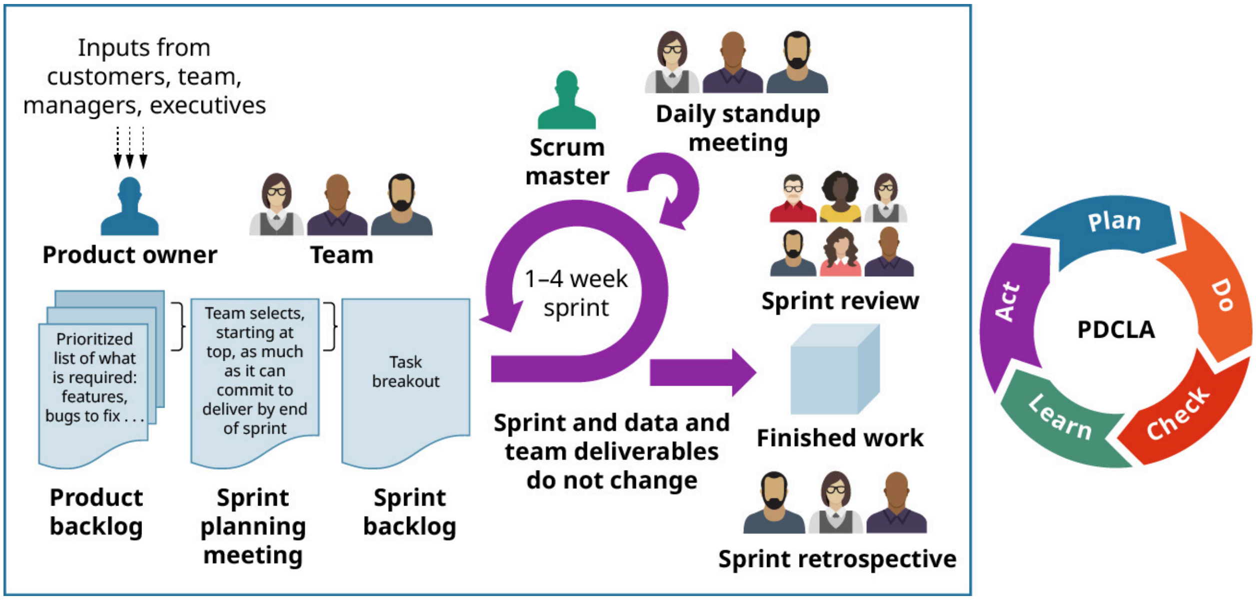


Figure 4.9 An Agile team manages the planning and prioritization of work to be undertaken toward a completed product, generally within a 1–4-week iteration. (credit: modification of work by Pietro Casanova, "Agile Processes: A Unifying Approach for the Future of Projects" (paper presented at PMI® Global Congress 2013 --EMEA, Istanbul, Turkey, April 24, 2013), Project Management Institute. https://www.pmi.org/learning/library/agile-approach-projects-market-globalization-5777)

CAREERS IN IS

Agile Project Manager

Agile project managers lead Agile teams and deliver projects using the Agile methodology. Managing projects with an Agile method differs from traditionally managed projects as the Agile project manager guides the team through dynamic, fast-changing, and sometimes volatile environments with a good deal of uncertainty to achieve project targets. The skills required for this role include excellent communication and organizational skills, effective critical-thinking, the ability to work well within a team environment, and a strong understanding of Agile and project management processes. These positions can be found in a variety of organizations but are generally housed in IS departments.

Another element of Agile project management is sprint planning. A **sprint** is a time-based period, generally between 1 and 6 weeks, that represents a delivery cycle during which the specified work is completed and reviewed. During these sprints, the team will have a daily meeting, often called a **stand-up**, generally between ten and thirty minutes, to discuss progress made and challenges encountered. The team will also discuss the design needs of the work, which may occur before or during the first sprint. Additionally, teams will break down large tasks into subtasks for each sprint. For each sprint, an Agile team identifies, based on the skills of its team members, the user stories it will work on during the sprint, and it estimates the time required for completion. For example, the team may decide on a two-week sprint, aiming to complete two coding tasks, two testing tasks, and two documentation tasks. After this, the user stories are prioritized accordingly.

During the sprint, the team members will actively work on their assigned tasks and resolve any issues needing to be addressed. When an issue arises during sprints, it is added to the backlog and prioritized with the work already maintained in the backlog. At the completion of each sprint, the team generally has a usable and workable product, ready for the stakeholder or product owner to review during a sprint review meeting. Teams may be able to see the amount of work remaining through the use of a burndown chart, or a graphical representation of the work completed in a sprint and the work remaining over time. The team has a postsprint review to identify challenges and opportunities for the next sprint cycle. This process continues until the backlog of work is depleted and the functional components of the product are completed. Once the backlog of items has been addressed, the team will hold a **retrospective meeting** where members will discuss the sprints in detail and areas of improvement to apply to future sprints.

Advantages and Disadvantages of SDLC and Agile Software Development

In determining how to approach systems analysis, the advantages and disadvantages of SDLC and Agile should be considered. Some aspects of the processes might be better suited for specific types of projects, while others may not. The flexibility required in the nature of today's business world and how businesses operate might require a hybrid approach to software development that includes aspects from both SDLC and Agile.

The structure in the SDLC approach can offer projects rigor, detailed documentation, a thorough examination of the risks and pitfalls in a design, and careful attention to budgetary considerations. However, SDLC is not designed for projects with a good deal of uncertainty in the beginning stages, nor is it suitable for projects in which unexpected changes might come up. This is where Agile software development's more fluid approach can be beneficial. Through a more iterative approach and with close collaboration with end users, the design can be clarified, key stakeholders can be involved, and unexpected issues can be systematically tackled. Agile has been criticized for its lack of detailed documentation and the unpredictable costs that can result from its focus on speed and flexibility. But by using a hybrid approach, organizations can mitigate these weaknesses and utilize the strengths of each approach to meet their needs.

Consider the scenario of developing the POS system for Fenner Street Boutique to see how the hybrid approach works in practice. With the ribbon cutting and website launch already scheduled, the business owner faces a tight deadline and is particularly concerned about staying within budget. Because the POS system will be crucial for inventory control, it needs to be up and running before the store opens. The SDLC approach helps by providing clear deadlines and documentation, ensuring the system is scalable for future growth, and keeping budget considerations in mind. On the other hand, the Agile approach allows the owner to stay involved throughout the process and adapt as needed, such as adding the finalized logo once it's ready.

Furthermore, as the owner is still deciding on the final inventory for both in-store and online items (including potential "online exclusive" products), there are uncertainties to address. Agile software development is ideal for handling such flexibility, giving the business owner a voice throughout the development process. In sum, SDLC offers the structure necessary to meet deadlines and budgets, while Agile allows the business the flexibility to make decisions as its vision evolves.

Roles and Responsibilities of the Analysis and Design Teams

Analysis and design teams may consist of several members using various tools and methods to create design-related solutions, such as designing a mobile application, building a website, or any other design effort. The size of the team will vary, as will its structure—from centralized design teams with hierarchical organization to flexible teams of contract resources. Both structure and size will be determined by the scope of the effort and the types of expertise needed. Table 4.1 lists the roles found on an analysis and design team.

Role	Responsibilities
Designer	In the early stage of software development, a designer creates and tests software solutions to improve on an existing system or to develop a new one. Designers may assume a general role on the team or may have a specialized role such as a product, visual (user interface), or user experience designer.
Systems architect	Systems architects are responsible for the technological and management aspects of the design; creating the hardware, software, and network systems; and working within multidisciplinary teams of experts to grasp the big picture.
User experience (UX) researcher	UX researchers conduct user testing to validate ideas slated for the design, collect user data, and track stakeholder feedback. This team member's responsibilities extend to gaining an understanding of user behaviors, needs, and motivations via focus groups, surveys, and interviews to evaluate how users make use of the design solution.
Systems analyst	These professionals' primary function is to detail the technical specifications of the system and lend their IT backgrounds to the technical needs of the team.

Table 4.1 Analysis and Design Team Roles and Responsibilities The members of an analysis and design team vary by organization and by project. These are common members and roles.

LINK TO LEARNING

There are many approaches to completing a feasibility study, which is an assessment of a proposed project or business venture that aims to understand its strengths and weaknesses and explores its technical, market, operational, and financial fitness. Suppose you are hired as a consulting systems analyst to provide services for a financial institution that is interested in expanding services into a neighboring state. It may be easy to assume that the feasibility study should have more of a financial focus than a technical one, but other areas of consideration (such as operational, environmental, legal) are important and can impact final decision making. Read this article providing some insight into how to create a feasibility study (https://openstax.org/r/109FeasbltyStdy) to learn more.

4.2 Defining the Business Problem and User Requirements

Learning Objectives

By the end of this section, you will be able to:

- Explain how to determine a business problem
- Identify the tools and techniques used to define user requirements
- Describe the consequences of incomplete or incorrect user requirements
- Apply what you have learned about defining a business problem and user requirements

Businesses are often challenged with finding solutions to problems affecting their operations, and such challenges can influence the overall health of the organization. Some problems are easily identifiable and readily avail themselves (such as an assembly line failure), while others require a more intricate analysis of the problem (declining membership, for example). In either case, before beginning any problem-solving process, it is important for a business to determine the exact nature of the problem it is experiencing and the extent to which the problem's effects have spread through the organization.

How to Determine a Business Problem

A **business problem** is any obstacle to business operations that causes variance in the expected outcome. These variances can have a significant impact on an organization's bottom line, affecting its ability to maintain healthy operations and sustain itself among its competitors. While variance or some level of uncertainty is expected in business, when variances occur, business leaders need to know how to effectively address them. Consider the scenario that occurred during a busy holiday season in 2013, when the CIO of Target was made aware by the company's security team of a security breach of its POS terminals in which the credit card information of customers was being compromised.[2] Let's suppose you are the CIO of a major corporation, and its network security is threatened by sophisticated malware. How do you determine a business problem, the extent of its impact, and the possible solutions that are timely, feasible, and responsive to the problem? You need to follow these steps to define the problem, determine and then implement solutions, and evaluate how the solution worked.

1. Define the problem: Defining the problem can be as simple as starting with general questions to further explore the situation. Asking questions may elicit or uncover the general problem and may help you to think through the problem from a critical lens. The "five whys" refers to an iterative interrogative technique that can be used to explore the cause-and-effect relationships underlying a particular problem, and it is an example of how to approach the process of defining the problem by asking questions. The technique was invented by the founder of Toyota nearly a hundred years ago, gained popularity in the 1970s, and is still used today to solve problems. The idea behind the technique is that asking questions may help you gain a deeper understanding of a problem. An opening question might be "Why is that a problem?" "Why did it happen that way?" or "Why did it happen now?" Subsequent questions are then posed to help further your understanding of the problem, such as: "What areas of the business is the problem affecting?" and "What business roles or teams are impacted?" In theory, asking continuous "why" questions to dig further into an issue should help to identify the problem by the fifth "why." To add further value, organizations may use techniques like this to engage the help of employees, stakeholders, and others in defining the problem, which can lead to a more thorough and effective evaluation process, provide individual value to team members, and result in an effective resolution—all means by which the business can build opportunities for its success.
2. Determine possible solutions: Once there is a good understanding of the problem, the process of determining possible solutions can begin. Using data collected when defining the problem plus the insights gained from those participating in the process, brainstorm potential solutions that may solve the problem. It is important to consider the "do nothing" option, along with its ramifications from a near- and long-term planning perspective. The solutions should consider cost, impact, time, resources, and other factors that qualify their viability as options.
3. Assess, select, and implement a solution: Review the options presented and weigh the pros and cons of each. For example, suppose the organization depends on a preferred piece of hardware that is delayed with an international supplier. Should hardware be replaced with a lower-cost, regional option that may not be as reliable, or should the organization wait for the supply to come in? The cost of waiting for the preferred hardware may be significant, but the regional part may pose a quality risk, causing the organization to make amends to save the relationship. The organization should select and implement the option that is the most feasible and viable the—one that delivers the most benefits with minimal disruption.
4. Evaluate the solution: How well did it work? When a solution succeeds, it is common to apply that solution to similar problems. But for those solutions that do not work out well, the process of defining the problem may need to be restarted, and solution options may need to be reevaluated. A different option may be selected to provide the desired result. As part of the closing process of a project, it is important to reflect on opportunities for improvement and catalog best—as well as next—practices. The key is to avoid making

2 Kevin McCoy, "Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers," *USA Today*, May 23, 2017, https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

the same mistake more than once and building on the solution that was successful through broader and deeper application.

Tools and Techniques Used to Identify User Requirements

Solving business problems requires understanding what is requested by the users or owners of the product/service and needed to support their business functions. The **user requirements** are aspects of a solution that are specified by stakeholders and needed to support specific needs and expectations of a business process or product. For example, in seeking a Human Resources Information System (HRIS), the users of this system (HR managers, HR support staff, organizational employees) may request features to manage hiring, employee performance evaluations, payroll, and employee benefits. User requirements are often recorded in specification documentation and can be further categorized as either functional or nonfunctional requirements.

A **functional requirement** is the feature or function of an application that is needed for the affected business area to accomplish its tasks. These may include business rules, transactions, administrative functions, audit, authentication, authorizations to external interfaces, and reporting functions. With respect to the HRIS example, a functional requirement may be a simple search function that involves using an ID number to search for an employee and, if found, returns results relating to that employee.

A **nonfunctional requirement** is an attribute of the system that enhances its functionality or operation. Nonfunctional requirements are often viewed as those items that describe the general properties of the system or how the system should behave and work. These may include performance, scalability, security, flexibility, operating constraints, usability, interoperability, maintainability, availability, and capacity. In the hiring example, HR managers would require that the HRIS system is secure from vulnerabilities and threats. They would also require that payroll runs smoothly and adjusts accurately for yearly tax updates, rates, and withholdings. All of these are nonfunctional requirements.

Requirements are generally determined by a team of individuals including stakeholder users, analysts, and/or IS team members with general knowledge and expertise about the system being designed or modified. Administering user observations, interviews, cross-functional meetings, questionnaires or surveys, documentation analysis, brainstorming, and interface analyses are methods used to elicit requirements needs from these individuals.

One means of storing this information is a **requirements traceability matrix (RTM)**. Generally a spreadsheet or similar, the RTM is used to record each requirement along with supplemental information, such as its type (functional/nonfunctional), description, objective, business need/justification, priority, department, and the status of its development. Many organizations also use this document as a testing reference to ensure each requirement has been thoroughly reviewed, tested, and confirmed. In addition, the RTM helps with the verification and validation of the requirements/needs and wants analysis.

Another tool used in gathering user requirements is a **design diagram**, which is a simplistic drawing or elaborate depiction that helps design teams as it is simple to understand, universally accepted, and easy to compare. It plays an important role in design presentations as they allow viewers to visualize systems, structures, and the relationships between them. There are, however disadvantages of design diagrams, including the time involved in creating them. Consultation with other stakeholders or further research may be needed to complete the design diagram, causing it to be a time-consuming process. As more specialized design software programs become available, design diagrams can be costly. Moreover, they can be misleading, inaccurate, biased, or confusing if they have been conceived incorrectly or are purposefully minimizing or highlighting certain aspects.

Some design diagrams can be generally categorized as maps, charts, or graphs, while others are specific in type and can provide a specific view of the data being presented. Some examples include:

- A **flowchart** is a diagram that displays sequential relationships between data, systems, programs, or processes. They are often used by technical and nontechnical persons to document, plan, and communicate ideas in a simple-to-understand visual format. Flowcharts utilize specific symbols, diagrammatic arrows, and connectors to aid in the visualization.
- User stories are explanations from the user perspective, usually written in an informal format, of specific systems functions. The components of user stories are referred to as the 3 Cs: cards (the user role, general task, and goal to be achieved), conversation (discussion with the development team in which users gain clarity about the user requirements), and confirmation (agreed-on acceptance criteria for satisfying the user requirements).
- An **As-Is/To-Be process map** details the "current state" and "future state," respectively, of a specific process or function within an information system. The As-Is process map details how things currently work, while the To-Be process map describes what should be done to reach the desired future state.
- A **use case diagram** is also a visual representation of system features that displays how specific users interact with the specific functions of a system. These diagrams usually contain the following components: actors (human or any external entity), a box representing the system itself, and directional arrows that show the relationships between the actors and the systems that indicate the flow of data, to and from the system. Figure 4.10 shows a use case diagram depicting the system setup of a boutique seeking to expand by opening a brick-and-mortar store and online store that use the same system. Customers (actors) would face different decisions based on where they were making a purchase. This diagram might be accompanied by the written use case, which would include specifics about the account creation process for an online purchase and the process for in-store transactions.
- A **context diagram** is a high-level diagram that visualizes a system or parts of a system and the environmental actors with which it interacts using diagrammatic arrows to display the flow of data. These indicate the highest level of interaction between the system and business processes.
- A **mind map** is a free-form depiction of ideas with branches displaying the flow of information and thoughts, and they are generally used for brainstorming.

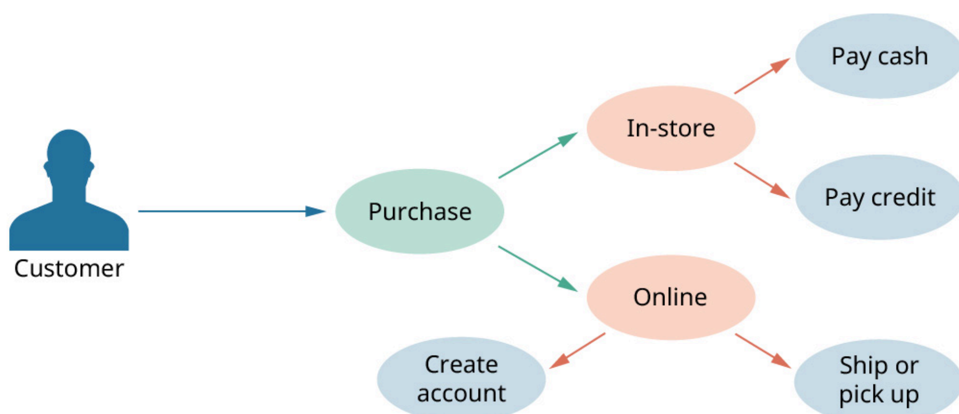


Figure 4.10 A use case diagram for a boutique would outline the various aspects of the system based on whether the customer was an online customer or an in-store customer. (source: attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

LINK TO LEARNING

A business requirements document (BRD) is a formal guide that gathers all the aspects of the business needs and details associated with a new project or program solution and its success, including the objectives, expectations, and the reasons why the company is in need of a solution. The BRD will help guide a team toward successful implementation of a solution that will meet the needs of the business. Review the recommended components, and access template examples (https://openstax.org/r/109BusReqDoc) to learn more about how to create a BRD.

Consequences of Incorrect or Incomplete User Requirements

The requirements-gathering process doesn't always result in a perfect set of instructions to address the business problem. Often, the RTM can be fraught with missing or incorrect user requirements, and this can significantly impact the delivery of a final product and may cause challenges for the project team working to deliver the product. Not only will there be associated costs (resources, regulatory penalties, delays to market), but the impact may include undocumented processes, conflicting requirements, communication challenges with end users, and a misguided focus on the visual aspects of the design instead of the functioning elements.

In the spirit of continuous improvement, systems analysts can iteratively address poor requirements by doing the following:

1. Do thorough research: Increase knowledge of the business problem by understanding the factors and driving forces contributing to the business need. Research should focus on the context in which the business exists and include both internal factors (like organizational culture and business processes) and external factors (such as market conditions, regulatory requirements, and competitors). Ask: Are other organizations experiencing the same business challenges or opportunities? What are other organizations doing to address this? The research may validate or refute the gathered requirements, or identify new requirements to consider.
2. Revisit the business problem or opportunity: Once the research is completed, use the knowledge gathered to revisit the business problem or opportunity. The situation may be viewed differently and can provide additional insight. Is the business problem or opportunity what was envisioned? Can the business problem or opportunity be spoken about more confidently to support the team? Can insights be offered that may support a more comprehensive requirements document?
3. Conduct requirements review sessions: Initiate sessions to review the requirements with all stakeholders. Feedback from these sessions may elicit additional valuable input. Be sure to include visuals in the review sessions (data maps, flowcharts, diagrams, reports) as they can often convey information with greater clarity.
4. Seek approval: Final review and approval from stakeholders and business owners may prove useful in addressing incomplete or missing requirements as well as validating the requirements gathered.

Consider how the requirements gathering process might be applied to establishing intramural competitions at a university, which are often student-led initiatives. A student has been assigned responsibility for their college's intramural sports leagues throughout the year. This involves setting up team registration, recording payments, keeping track of scores, setting up tournaments, and reserving space on campus for games. The leagues have been getting more popular and the old way of managing the process is no longer as effective. A faster, electronic process is needed. Also, as students graduate, there needs to be a plan in place to train and transition to a new manager. Having an app or similar type of system to manage the aspects of the league would be helpful. The students would need to get help from both the IT and athletics departments. It would also be important to get feedback from team captains or coaches as to whether they would use the app to register teams and track their progress through the season. Some tools that might be useful include a design diagram and a flowchart. The flowchart can be used to show how a team will work its way through the system as the league progresses to the eventual championship tournament game. Finally, a key consideration is cost. There is a very limited budget to develop the application, so it would be ideal to be able to access existing technologies in use at the college. These are just some of the considerations when designing the intramural app and how key stakeholder input can be incorporated into the final product.

GLOBAL CONNECTIONS

Requirements Gathering in Globally Dispersed Teams

It is increasingly common for organizations to operate globally, with teams and services dispersed internationally. When teams are spread globally in different locations, it may complicate the requirements gathering and software development processes, leading to inefficiencies and cost overruns. Often, organizations may opt for Global Software Development (GSD) services. These services enable knowledgeable workers in various parts of the world to develop software solutions for organizations. Unlike traditional teams where individuals are colocated and tasks and activities are distributed to achieve a common goal, GSD teams are virtual and rely heavily on communication technologies to develop software. There are some challenges associated with GSD services, such as lower productivity and challenges in communication. To ensure that the GSD process is effective, coordination across virtual teams and project leaders is needed.

Defining a Business Problem and Determining User Requirements: Case Study

Dr. Singh has had a thriving medical practice, Hometown Physicians Group, for several years and is looking to expand her practice by opening another location in a neighboring town within the next six months. Dr. Singh is concerned that her current practice is fraught with challenges that she does not want to carry over to the new practice location. These challenges include manual billing and accounting practices; the use of multiple operating systems, hardware, and software systems; lack of security as staff use personal devices to record patient visit information; and older patient records in paper files. Many of these challenges can be resolved with a new electronic health record (EHR) system. Such a system could also help ensure the office is in compliance with medical privacy regulations and using it may improve the practice's compliance with industry regulations. Lastly, Dr. Singh would like her patients to be seen in either office.

Additional information about Hometown Physicians Group:

- There are twenty-five additional employees, including clinicians (doctors, nurses, and medical assistants) and support staff (billing and accounting, practice management, and reception).
- The office must upgrade to a new EHR as the relationship with the old one will be ending in six months.
- The transporting of manual files between offices needs to be eliminated, as does the practice of using personal devices for patient recordkeeping.

Assume the role of the designer and user experience researcher in this scenario. Recall the designer's role is to provide guidance in the early stages about the system that will meet the business needs. The user experience researcher is focused on making sure the system design meets the needs of the stakeholders—in this case study, Dr. Singh and her associates. Think about the process to accurately define the problem and which tools could be used to visualize the problem and the system for Hometown Physicians Group. You might consider whether there are other key stakeholders who might be important to include in the conversation. Consider the following as you work through the design process:

- How would you approach the requirements gathering process?
- Who are the stakeholders involved and how would you engage them in the analysis?
- What tools would you use to understand the business processes and the opportunity presented?
- What questions would you like to ask Dr. Singh that would assist you in your work?

Let's begin by defining the business problem. Keep in mind that the circumstances do not need to always be problematic. Instead, as is the case here, Dr. Singh has a new opportunity to expand the practice. This opportunity might involve some challenges, but sometimes the use of the words "business problem" implies a negative situation, whereas this expansion is positive. Dr. Singh has provided initial information to give context to the existing issues in the office's current operations and how they may present additional challenges in the new business model. Begin with the five-whys method or other appropriate questions. For example, you might ask why the current billing system is a challenge for the office staff. You can also probe into how the different operating systems currently present issues.

In addition, it would be important to engage Dr. Singh in a conversation about the other stakeholders who need to be included in the initial design stages, and in the testing and evaluation phases of the project. This could be done through a requirements review session. During these initial stages, tools such as the RTM, flowcharts, and use case diagrams could help you visualize the overall business problem and the system requirements. Moreover, it could be helpful to use a design diagram to show Dr. Singh how the current system functions and the relationships that currently exist.

Once you feel confident in the business problem definition, move on to the next stage of determining possible solutions. During this phase, you can continue engaging with Dr. Singh and the office associates and utilizing some of the tools mentioned. You will want to address the user requirements (functional and nonfunctional) in the proposed solutions. Try to offer a couple of solutions, and for each be sure to include information such as cost factors, time, and training required to implement the solution. This is a good time to revisit the RTM to ensure that the proposed solutions meet the needs and wants of the practice. You could also consider creating a new design diagram to show how the proposed solutions differ from the existing system.

Next, the project would move on to the selection and implementation phase. During this stage of the process, the proposed solutions are evaluated, and a final solution is selected. It is helpful to generate a pros and cons list for each and to engage the key stakeholders in the conversation. Ultimately, you should implement the option that is the most feasible and viable for the office, one that gains the most benefits with minimal disruption.

The final phase is to evaluate the solution. This phase is likely to not have a specific endpoint. You might deploy tools for Dr. Singh to evaluate the functioning of the system on her own. But initially, the design team will want to evaluate how the system functions to meet the user requirements and the needs of the office during the transition. As the users interact with the system, it is likely that the need for improvements or changes will arise. You might consider establishing a process by which these system changes and improvements can be communicated to the design team. The feedback could be provided as the issues arise or be compiled and shared with the team on a regularly scheduled basis, such as quarterly. The goal is that once the system is operational, feedback from the users is solicited to evaluate the efficacy of the system in meeting the needs of the medical office. This evaluation stage is crucial and should reflect back on the business need that was identified in the early stages of the project.

This case study provides a general framework and some factors you might consider as you work to develop your solution to this problem. You might have other ideas on how to approach the problem, uncover user requirements, and produce creative solutions.

CAREERS IN IS

Analyst

Analysts are the most common professionals engaged in defining the business problem or opportunity as well as leading or managing the requirements gathering process. This position’s title has many variations, including business systems analysts, systems analysts, and different versions of software engineers. These roles can be found in all areas of a company, including IT departments. Common skills required for these roles include being knowledgeable about business analysis, communication, requirements gathering, analytics, and software (Microsoft, Azure, Python, R) or tools used for documentation. Higher-level educational degrees, certifications, and experience will contribute to higher salary earnings.

4.3 Technical Design Methodologies and Practical Applications

Learning Objectives

By the end of this section, you will be able to:

- Explain systems design principles and networked architecture
- Identify systems designs for enterprise network architectures

The launch of a new company, or the decision to expand an existing business into a new area, are organizational shifts that require new systems. The design of those systems, and their architecture needs, will be most successful when planned using established design principles and best practices. Consider Dr. Singh and the medical office expansion of Hometown Physicians Group. The addition of the new office with the new billing and electronic records system has worked out well. Both offices are functioning as expected, patients can be seen in either location, and patient records comply with current electronic reporting requirements. As part of an outreach effort, Dr. Singh is considering adding a monthly walk-in clinic for vaccinations at the local community center. This would further complicate the system that is currently in place as it is not set up to track nonpatients or to accept government-sponsored health-care programs. The latter capability would need to be addressed and incorporated into the system as the practice can be reimbursed for some expenses through the government-sponsored health-care program. One additional complication is that the program requires specific reports and data to be submitted quarterly through the state health-care program portal.

With these capabilities, Hometown Physicians Group would provide an important service to the community, serve as a source of clinical hours for those studying to be health-care professionals, and contribute to a health-care issue that Dr. Singh is passionate about. To accommodate this new venture, the current system will require additional design work.

System Design Principles and Networked Architectures

After gaining an understanding of the business problem, completing a systems analysis, gathering user requirements, and generating design diagrams to potentially address an organization's business opportunity, it is time to begin the next phase. The **system design process** determines and defines the architecture, interfaces, and data for a system that can satisfy the specified requirements. There are several general guiding principles that govern good system design, including:

- Simplicity: Simplifying the design and system solution is preferred as overcomplication can require more work, time, and sometimes leads to solving problems that do not exist.
- Clarity: Designs should be clear and easy to use. Be mindful of users who will interact with the product. What type of experience would an end user want to have while using the product? Avoid or minimize complexity where possible.
- Core functionality: The main or core functionality and its interrelated parts are the most important. Additional system features and details can wait.
- Scalability: Does the solution have the capacity to respond to organizational change—that is, handle additions or reductions of users, clients, products, processes, services, data, as well as an evolving business landscape? Where does the company want to be in the next few years, and how would that impact scalability needs? These considerations should be appropriately addressed within the solution to minimize any constraints on organizational change.
- Reliability: The design and system solution should be reliable when it functions in accordance with its designed specifications, with no or minimal failures during the specified time of its use.
- Security: How secure is the system from external or unauthorized use or threats? A system is deemed secure when authorized users can access it and when all measures to control and safeguard the system are in place.

ETHICS IN IS

ACM Code of Ethics

All those involved with the systems analysis and design team are expected to maintain ethical standards to facilitate a relationship of trust with the customer. There are eight principles focused on the following: public, client and employer, product, judgment, management, profession, colleagues, and self. These principles were designed to guide decision-making for computing professionals, with a focus on integrity in decision-making and advancing the public good. Just as other professionals such as attorneys and doctors have codes of ethics to protect clients and patients, the ACM code of ethics was established for computing professionals to avoid unjust harm, promote honesty and fairness, and respective privacy to protect customers.

You can find a full description of the Software Engineering Code—ACM Code of Ethics and Professional Conduct (https://openstax.org/r/109ACMcode) at the Association for Computing Machinery's website.

Network architecture is concerned with the fundamental principles and concepts that underlie the design and operation of a network. The **network architecture** is a top-level view of the system that defines the equipment in the network and the interaction between the equipment . For example, in your home you might have a printer connected to a network/LAN or the internet. In this case, the network architecture includes your computer/laptop, the printer, the modem, and the router. It could include additional equipment, such as Bluetooth devices or your mobile phone.

The **network design**, in contrast focuses on the specific implementation and configuration of a network to meet the requirements of a particular organization or application. Network designs can be created using various types of design models and tools. These may include logical and physical designs, prototype designs, or computerized system designs.

Logical and Physical Designs

Designs of systems can be logical or physical, and as these designs are developed, it is important to clearly represent the information presented in both. A logical design illustrates how data is logically presented and flows through the designed system. The focus of logical designs is not on the physical attributes of the design, but on the business needs of the organization and the information gathered from stakeholders about the business problem or opportunity. Logical designs incorporate the business processes needed to visually represent these activities, the flow of data, and the relationships between them—all of which will be later used to create the physical design.

The goal of logical design is to create a high-level representation that is independent of any specific software product. Logical designs can take many forms. One is the **entity relationship diagram (ERD)**, which is a structural diagram used in logical database design that serves as a visual representation of the data flow and its relationship among people, objects, events, places, or concepts. ERD models are composed of entities (something that is definite and uniquely exists, such as a business, college course, or person), attributes (characteristics or traits of an entity), and relationships (interactions between two or more entities).

For example, Figure 4.11 shows an ERD of a doctor's office. Entities are uniquely identified in rectangular boxes—physician treats patient, physician orders treatment, physician refers to specialist, facility treats patient, and so on—and directional lines with symbols represent the relationship of the connecting entities.

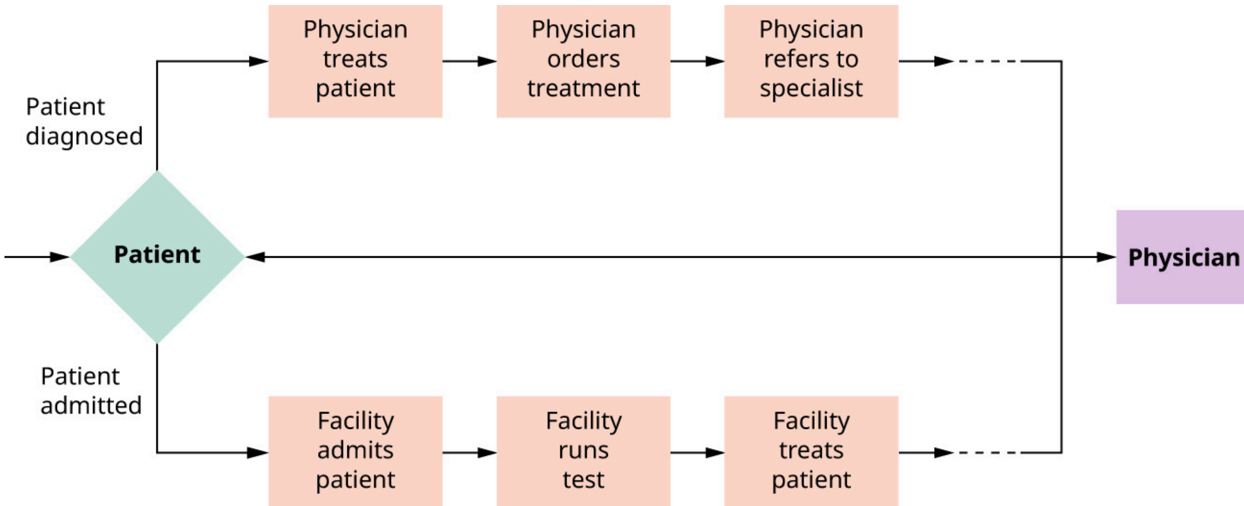


Figure 4.11 An entity relationship diagram provides a visual representation of a system or process, allowing users to see relationships between entities and their attributes. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

An additional output of the logical design may be the **data dictionary**, which details the category names and supporting properties of the data used in the database. The dictionary is usually organized in table format, and the general properties for the table may include the column name, contents, number/type of characters, required/mandatory indicator, and any other aspects of the data that support the logical design.

A physical design utilizes the completed logical design to create a concrete, physical system with specific hardware and software components, detailed systems diagrams and layout, and the requirements for each component. Physical designs allow teams to visualize the physical structure of the system and its supporting components and characteristics. During the physical design phase, the data gathered during the logical design phase are input into the tables, columns, indexes, and places where further details can be added. The physical design can be built to optimize query performance, data maintenance, or whatever functions the business needs.

CAREERS IN IS

Systems Designers

Systems designers are specialized professionals who support the analysis and design of information systems. These roles require having technical and analytical knowledge, expertise with software or tools used for documentation, and also possessing communication, leadership, and problem-solving skills. Systems designer roles are generally found in IT departments—with higher-level educational degrees, certifications, and experience contributing to higher salary earnings. Job titles with similar career paths include systems/computer engineer, IS specialist, and software developer. If you are interested in additional information about a career as a systems designer, you can check out the Indeed (https://openstax.org/r/109IndeedCareer) career guide.

The Data Cycle

The **data cycle** refers to the different stages that data undergo while they exists in an organization's system, from its initial generation onward.

- Creation: During the creation stage, the team addresses the different methods by and inputs through which data are created or captured. Data may exist in different formats—such as Microsoft Word, PDF, and SQL—and it is important to identify these data types in considering how to manage this data. For example, your data may enter the data cycle via manual entry wherein authorized users input information directly

into the system. Data may also be captured through an import mechanism from an external source. This method is widely used in organizational acquisitions and transitions to maintain the historical components of data and to continue current business processes. The capture may also be generated from other input sources or devices used throughout the organization.
- Storage: Once the data have been created or captured within the system, they need to be stored for future retrieval, use, and reference. The security of the data along with backup and recovery functions are needed to ensure the data are secured and retained for the organization's use.
- Use: The data usage stage provides an understanding of how the data are used to support business functions. How are the data processed, modified, and saved? Where is the audit trail of data manipulation, and how should it be maintained?
- Sharing: The sharing of system data is another key aspect of the data cycle. The data should be made available so it can be shared internally (in which case, it could include reporting and data analysis purposes) and externally (in which case, it might include sharing data for regulatory reporting requirements).
- Archival: Data archival is the process of transferring data to a nonactive environment for storage, a location other than where the system's daily use environment exists.
- Destruction: Data destruction is needed as data grows to a volume that is no longer feasible to maintain. Generally, the destruction or purging of data occurs from the archival location, and every copy of the data is removed within the guidelines of the organization's regulatory retention period.

Prototype Designs

A **prototype** is a design approach wherein systems designers and users create a small-scale representation or working model of the solution. Prototypes are generally created using an iterative development process, or a series of continuous planning analysis, implementation, and evaluation steps that lead to a design that has increasing functionality and increasingly meets the user requirements. Prototypes also enable users to modify or make interim changes through to the completion of the final product. In addition to the flexibility that prototypes offer, their other benefits include:

- early detection of functional problems
- increased user participation, engagement, and team collaboration
- increased satisfaction with the final product
- greater savings of time and money associated with rework

Creating a prototype does, however, have its drawbacks. Prototypes can be costly to complete and time-consuming to develop. Often, the features included may differ from the final product, and this can be misleading for the stakeholder as it does not provide an end-to-end functioning product. Prototype development also lends itself to rework due to changing business requirements.

Computerized System Design

Use of computers to assist in the design process, including the creation, development, modification, or optimization of design systems is called **computer-aided design (CAD)**. Sometimes called computerized system design, CAD is increasingly used to optimize resources and maximize time to delivery. Designers, engineers, and other technical resources frequently utilize CAD in situations where its ease of visualization, level of detail, capacity for specialization, and ability to optimize products and render a physical product can assist in the design process.

Input/Output Control

In information systems, input/output control falls under the systems design process. An input is the raw data that are processed through the functions of the system. Inputs are controlled by the directives used to submit responses into the system by the user, producing an output according to the system logic. Systems designers create input forms and screens that have quality considerations and that focus on the user experience. These considerations should provide users with the ability to move about the screen to different fields, confirm the accuracy of data entered, and capture the necessary data according to the requirements of its intended use. In Figure 4.12, the inputs of the hiring system (such as résumés and recommendations) are processed according to the system's logic into an output format (a decision to hire a candidate). The outputs are synthesized through the feedback loop to enhance the hiring process. For example, job performance and satisfaction data are fed back into the system to better analyze potential candidates based on the likelihood of performing well and being satisfied with their job. Certain demographics and experiences as found on the submitted résumés might show a trend in terms of performance and satisfaction. The feedback provided through the system can then be used to better filter potential job candidates and increase the hiring efficiency and possibly reduce turnover.

An output is the information the system delivers to users—in other words, it is the data resulting from the inputs being processed according to the system logic. System designers consider several factors that meet the user requirements. The outputs need to be the right output, quantity, speed, and accuracy. In the hiring example, the output from the system is a candidate to fill the open job position. Other outputs from the system are job performance and satisfaction metrics.

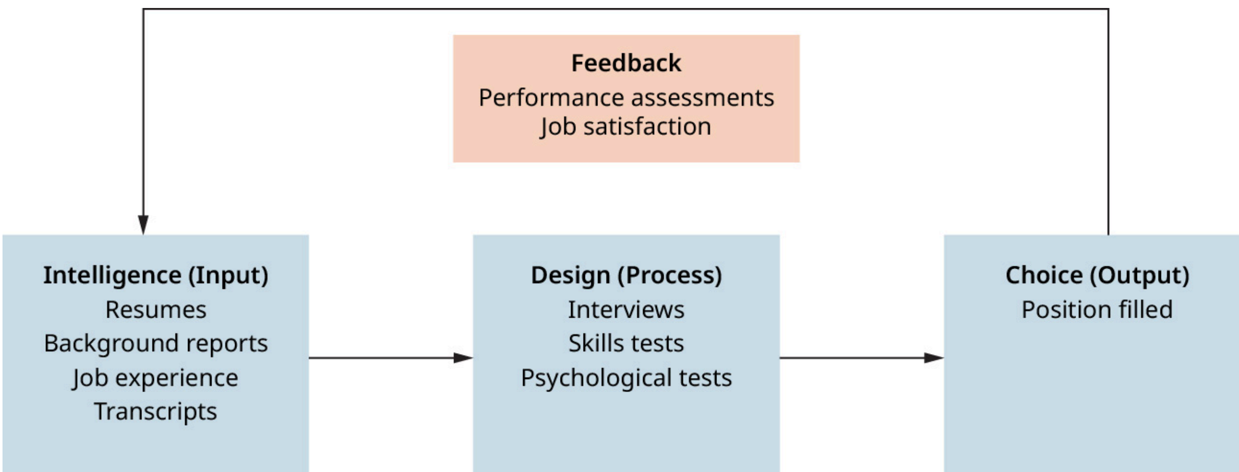


Figure 4.12 The inputs of the hiring system are processed according to the system's logic into an output format. This is a continuous process as new inputs are added to the system for processing. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Systems Design Task List

A **systems design task list** provides a road map through each step of the design process, allowing teams to have an organized workflow and make informed decisions at each step. A well-crafted design system improves the efficiency of teams and improves the speed of product delivery. These guidelines walk through the steps for creating a systems design task list:

1. Define and document design processes: Create clear and concise documentation defining the guidelines for system behaviors, standards, attributes, accessibility, and any other relevant information to ensure the design is user friendly and sets team expectations for the end product. Identify the technologies, system elements, and physical interfaces that will comprise the new system. Document the strategy to include a review of the user requirements for the system functionality.
2. Identify design characteristics: Define the architectural components relating to the system, ensuring they are able to be implemented. Create a shared language and vocabulary—for example, words, behaviors, images, phrases—to ensure consistency with the design elements as well as consistency within the team's shared experience in creating a unified user experience. Define and document the design characteristics for each identified component.
3. Assess alternative design options and finalize design decisions: Evaluate alternate design options based on similar, parallel, or new developments in theory and practice that may be feasible to implement as an

alternative to the identified system. Be sure to include those components at risk of becoming obsolete as the system is being built. Document the rationale for all options presented. Finalize and document the agreed-upon solution to include major hardware, software components, interfaces, subsystems, and dependencies. Revisit the preceding steps and adjust documentation as needed.
4. Build and manage the design: Design the solution to include major hardware, software components, interfaces, subsystems, and dependencies. Ensure that accessibility and inclusivity standards are included.
5. Review and implement the system design: Review the system design to ensure it meets the approved user requirements, engaging system owners, users, designers, and other stakeholders in the review process. Provide training for all users and system support staff to ensure proper use, support, and maintenance.
6. Measure the success of the design system and continue making improvements: Capture user feedback and evaluate the data received using metrics designed to measure its effectiveness and efficiency. Apply continuous improvement processes to address user feedback and system updates and changes.

Systems Designs for Enterprise Network Architectures

The **enterprise**, a term used to refer to as a business, organization, or company, is composed of a technical **network** or system of interconnected computers and other devices that allow for the exchange of data and information (such as files) and the sharing of resources (such as printers). Users are connected through devices and communicate via standard internet protocols. The **enterprise network architecture** refers to the structure and layout of an organization's network. Enterprise network architecture designs also reference pertinent business functions and provide insight into the overall technical architecture for the business, including the dependencies and connectivity of various applications. The goal of network architecture and its supporting design is to identify the most efficient way to transfer data from one hardware point to the other. Enterprise network architectures are composed of communication protocols along with local area and wide area networks (LANs and WANs), network devices (routers, switches, storage), end endpoints (servers, mobile devices).

There are several ways to design a network architecture, and selecting the right design should be based on the goals and requirements of the **network protocol**, that is, the set of rules and guidelines that determine how the data are exchanged between network devices. There are two broad types of network architecture: peer-to-peer and client/server. In **peer-to-peer (P2P) architecture**, the computers on the network are all given the same opportunity to use resources on the network. There is no central server for file storage, and network resources are shared. With **client/server architecture**—otherwise known as tiered—there is a central computer (server) that operates the network and allocates resources to the equipment connected to the network.

A key characteristic of a peer-to-peer network architecture is its decentralized nature. As shown in Figure 4.13, there is no central server through which the devices communicate directly. Each of the connected devices assumes equal capabilities and responsibilities, hence the term *peer*. This type of architecture is often used for smaller networks, like those in a home, and are highly resilient—even more than a centralized network—to the compromise of threats.

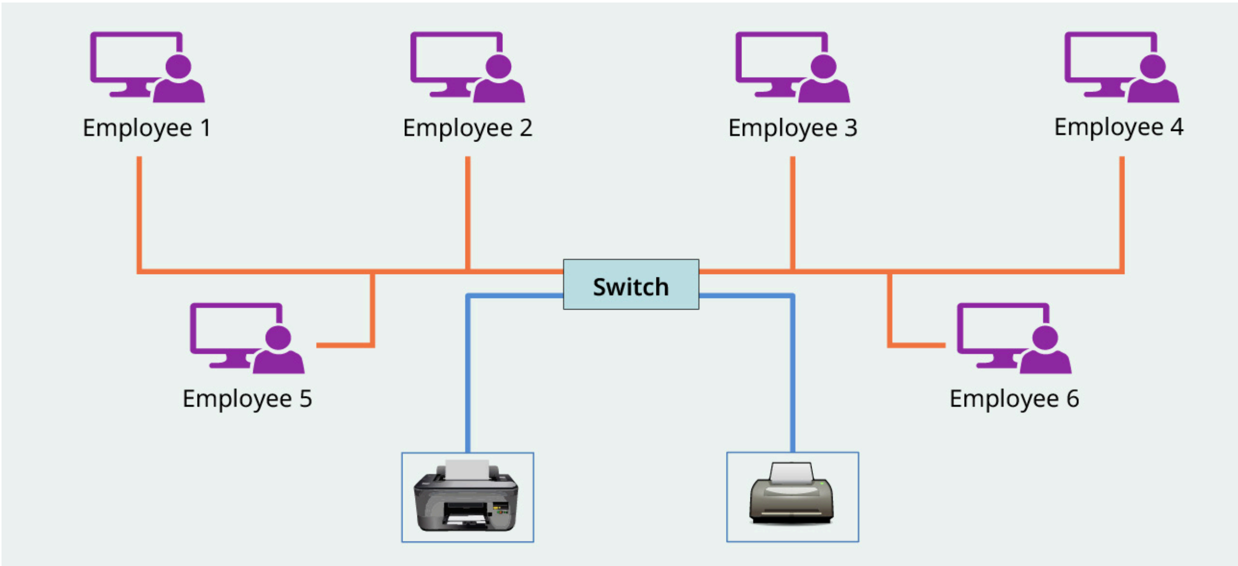


Figure 4.13 Each connected device in a peer-to-peer network assumes equal capabilities and responsibilities, and there is no central server supporting direct device communication. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

As shown in Figure 4.14, a client/server network is composed of servers and connected client machines—and thus considered a centralized network. Servers provide services—generally client requests—through their vast processing power. Client/server networks are associated with larger, more extensive computer networks utilizing WANs.

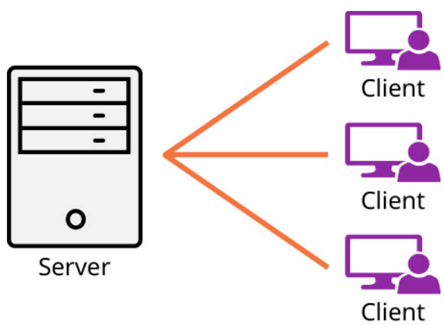


Figure 4.14 Client/server architecture is a centralized network composed of servers and connected client machines. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

GLOBAL CONNECTIONS

5G Technology's Global Reach

The fifth generation mobile network, or 5G, is the latest iteration of a global wireless standard. This 5G technology connects people, places, and things, including devices, machines, and objects. It provides increased availability, reliability, and network capacity, allowing for quicker service delivery to users. Increased network capacity allows for the maximum amount of information to be transferred at any given time and considers volume, traffic, utilization, and type of data. 5G became available in 2019 when most phone manufacturers began using the technology commercially. It is widely expected to expand beyond the sixty plus countries currently benefiting from the service, and it is also expected to extend beyond the mobile device industry, spreading into the automotive sector and others as well.

4.4 Designing for Mobile Devices and Other Design Considerations

Learning Objectives

By the end of this section, you will be able to:

- Explain user-centered design
- Identify special design considerations for mobile apps and social platforms

Designing mobile applications and social media platforms focuses on creating intuitive and engaging experiences by placing the user's needs, preferences, and behaviors at the center of the design process. Keeping users in mind ensures that apps and platforms are not only functional but also provide seamless and enjoyable experiences across different devices and user contexts.

User-Centered Design

Businesses increasingly recognize the need to incorporate stakeholder feedback into the design process, which reflects a shift from traditional design and development practices. A way to meet this need is to incorporate **user-centered design (UCD)**, an iterative, or stepwise, approach to development that considers the user's needs, behaviors, and preferences. UCD aims to positively influence user experience, gaining user loyalty for continued use of the product. In short, the user is placed at the center of the design process and the user's experience is factored into decisions where the business looks to align business practices and stakeholder research to create a design that aligns with the end user's needs. Applying user feedback to guide the design process not only strengthens the output of the design, but it creates a relationship with the user. Consider some best practices for how to implement the UCD approach:

- Define the business goal: To arrive at a final solution, businesses need to define their organizational goals. These goals set the direction of the design process. What are the strategic goals of the business? What are the targeted outcomes (in the short term or long term) of these goals? How will the design of the business reflect these goals and increase its socioeconomic and financial value? How does the system user fit into the strategic goals of the business and how will the system reflect that relationship? These decisions should also consider the market forces that will help shape the design. Namely, the organization should identify its target market, the intended users of its product/solution, and its competitors.
- Understand users and align business goals: The customer is the driving force of the design as the customers or end users will ultimately support the final solution. Therefore, having insight from the user's point of view is essential and foundational to UCD. This insight can include the user's needs, abilities, and constraints—each of which may impact a user's ability to fully interact with an information system's design. Consider the task of designing a website for a client. To meet the needs of users who might have specific challenges or differing abilities, the site might incorporate variable font size, color options, or larger buttons. Anticipating the user's tasks (current and future) is key for insight into the user's abilities and the challenges users might face when using the tool.
    - Do thorough research. Initiate interviews, focus groups, surveys, and other types of customer research methods to solicit user responses. Invite users who may provide insight into different roles or functions of the design. Consider assessing who will use the website, the environment, how the user feels when using the design, and their needs, abilities, and limitations. Gather and analyze the data using analytical tools and analytics as the data will drive decisions for the design. Learn as much as possible about the users in order to craft a product that fits their needs.
    - Evaluate the business needs and requirements. Identify and engage stakeholders to further understand your organization's goals, constraints, regulatory requirements, and budget considerations. Determine how to create the design and incorporate the data received from surveying users. Decide on the metrics that will be used to measure the success of the design.
- Generate the design solution and evaluate: Create a total solution that incorporates the user's feedback. Explore design tools for web design such as wireframes, user stories, mock-ups, and diagrams to provide

a vision of the full user story, leveraging business requirements and stakeholder feedback. Test the design end to end, re-creating the user experience. This process lends itself to the **iterative**, or circular, nature of UCD, namely, the cycling practice of building, refining, and improving a product, project, or initiative more than once. Be sure to account for and validate all the business and user requirements. Evaluate the design utilizing the identified metrics.

- Continue to refine: Continue to involve the user throughout the design process, refining the design as needed to assess its **usability**, a quality-related attribute that refers to a system or interface's ease of use.

A popular social media platform, Instagram, provides an example of this iterative process. Launched in 2010, Instagram provided a means for people to connect through photos and until 2012 was only available as an iPhone app. The app grew in popularity, prompting the platform to evolve as users interacted with each other and with the app itself. The first evolution was incorporating the hashtag (#). The hashtag was already in use on X (at that time, Twitter) to cluster similar posts and provide a searching mechanism for similar content.

Another addition was integrating Android capability, which led to an entirely new group of Instagram users. Eventually, the app incorporated ads, and it replaced the chronological order of the posts with an algorithmic order. As the user base increased and its needs became more apparent, business pages were developed, plus the ability to add a "story" and multiple pictures in a post.

Subsequent developments included "reels" and business Instagram shops. All of these developments and new opportunities came about through the implementation of UCD—specifically, the use of tools that aimed to better understand how users were interacting with the system. Instagram, much like other social media platforms, is expected to continue to evolve as user needs change.

Special Design Considerations for Mobile Apps and Social Platforms

Accessing applications via mobile devices has increased as technology has literally shifted into people's hands. The marketplace for mobile applications is crowded with all types. When considering how to approach design and development for mobile application use, recognize that applications differ in function and purpose based on their user bases. Despite their variability, mobile applications generally belong to one of the following categories:

- Social media applications: Social media applications allow community-based sharing via communication and collaboration. These applications lend themselves to connecting community members with shared content, expanding social networks. Users are driven to check in on such apps almost daily. YouTube, a popular social media platform, receives 2.6 billion users per day, and generated $29.2 billion dollars in 2022.[3] Other popular social media applications include Facebook, TikTok, and WhatsApp.
- Games and entertainment: The gaming and entertainment application space has expanded as accessibility includes mobile devices, computers, televisions, and game consoles. These interactive applications house activities related to leisure and fun. They are where content creators, marketing professionals, and artists collaborate to create an enjoyable interactive experience that generates revenue. Popular applications include Netflix, Hulu, Disney+, and Xbox Game Pass.
- Lifestyle: Lifestyle apps support and define aspects related to a user's lifestyle. For example, users who watch HGTV can now access the HGTV application to watch shows they missed, get exclusive content from hosts, and even enter sweepstakes. Other lifestyle applications include VRBO, Expedia, and Uber. Health-care applications can also fall under the lifestyle umbrella. Many health-care organizations are incorporating services via mobile technologies due to their ease of use, convenience, and reduced administrative costs to the organization. The health-care insurance provider Humana, Inc., is an example of a company using AI to improve operational efficiencies via mobile technologies.
- Productivity: Productivity applications (such as Microsoft Office, Docusign, and Calendar) allow users to manage tasks efficiently and effectively, leveraging the application's speed and convenience. Thanks to

3 Mansoor Iqbal, "YouTube Revenue and Usage Statistics (2025)," Business of Apps, updated January 22, 2025, https://www.businessofapps.com/data/youtube-statistics/

such applications, users may be able to handle basic banking transactions or sign an important document from a variety of locations or devices.

- News and information: News and information applications allow people to stay connected to current events by presenting news and information in unique formats that appeal to their users. For example, the Bleacher Report provides sports-related news and analysis, while Flipboard allows users to receive news and analysis on sports, politics, international relations, and other topics.
- Utility: Utility applications such as Calculator, Flashlight, and Weather may be preinstalled into a mobile device, generally serving a single, quick purpose.

Today, many users of technology need to access websites, software, and applications on various platforms. For example, employees who work from home may access a work software program via their tablet rather than their desktop computer in the office. Social media users often access their accounts through their phone, but they might also want to interact with an app through their smartwatch. It is important during the development process to design the system so that it can meet the user requirements on various platforms with nearly the same functionality. Specifically, website developers must incorporate making sure the website displays correctly on a mobile device into the development process.

Effective systems offer a seamless user experience between devices and platforms, which means that the functionality of the system is consistent for the user across various devices (such as phones, tablets, and personal computers) and platforms (like Android, IoS, and Windows). In some cases, users appreciate when applications are connected and integrated into other applications or software. This often occurs with products within the same company such as with Meta, who owns Facebook and Instagram. When a user changes their profile picture in one application, it is automatically updated in the other application. This can also occur with integrations of systems that are not under the same company. For example, payments held in an Apple Wallet on an iPhone can be integrated into a wide variety of shopping applications, and often that information is saved in the shopping app so the user does not have to enter payment information each time. These are just a few examples of how systems design has become more complicated over time as technology has changed and user needs and requirements have evolved.

These are a few practical design considerations for developing mobile apps and social platforms:

- Purpose and goals: Start by defining the purpose and goals for the application or platform. Do sufficient research. Discover the latest trends in design that may boost usability.
- Simplicity: Simple, functional designs with pleasing visualizations often generate buzz and increase the number of return users. For example, a good design might incorporate a color palette, features a status bar indicator to visually display the user’s progress, and directs the user to the next step through prompts.
- Reliability: The design should be reliable, meaning users should be able to access it successfully 24/7. To support this reliability, it should meet relevant speed and consistency standards. One dimension to consider is the data network architecture and infrastructure. In addition, review the policies of the mobile apps and social platforms to guard against misinformation (inaccurate or false information) and disinformation (false information given with the intent to mislead).
- Friendly navigation: Mobile app designs are most successful when they can be accessed well with friendly navigation. Users should be able to navigate the site’s functions via their fingertips, voice commands, or similar simple manners.
- Platform compatible: Consider different platforms in the design to create a seamless user experience. What works for iOS may not work for Android as the user interface may differ. Functional elements should be minimal and consistent with the website, as this builds trust among users when they access the application in either setting.
- Social media integration: As users become more inclined to share information with others in their communities and networks, social media integration may be a function that raises the design to another level. Here are some questions to consider while integrating social media into an application: How well does the application integrate with some of the popular social media applications? Would users want to

play games or compare outcomes with their friends and share the results on social media? How would this functionality expand the reach of the application and its use? What types of push notifications or social media application alerts would users need to have an optimal experience?
- Financial: There is a broad range of money needed for mobile application development as features such as push notifications, real-time updates, and third-party integrations may cause significant variations in expense. These costs can range from $10,000 to $500,000, and projects can sometimes involve many years of development.

LINK TO LEARNING

Read more about haptic technology that goes beyond the use of finger navigation (https://openstax.org/r/109HapticTech) at the Smithsonian Magazine website.

GLOBAL CONNECTIONS

Messaging Apps Fill Global Gaps

People increasingly want the ability to connect with their communities wherever they may be physically located across the globe. However, compatibility and coverage from carriers and service providers can pose challenges. Messaging applications emerged in the mid-1990s in response to this international need, and they gained in popularity because they provide an alternate communication method—via a user's mobile device—that is consistent with how people want to use technology to connect. Facebook Messenger, WhatsApp, Google Hangouts, and BOSS Revolution are examples of such applications. To use them to communicate, the user and receiver must have the application downloaded or be able to access it via a web browser. These apps are cost-free and continue to advance in their technological capabilities, bridging international communication gaps.

Guidelines for Mobile App Design

A good mobile design reflects the process undertaken by the development team, which ensure that the final design is not merely an acceptable product for stakeholder use, but also one that supports a stakeholder need and fosters continued use. Developers should also consider the impact of globalization on mobile app design, both in terms of international regulatory standards and user needs. This might include offering features that allow the user to select a language for the interface, and incorporating elements that are not regional or specific to a single culture or ethnicity. The following guidelines should be considered when designing a mobile application:

- Strategy development and planning: Strategy development is a major first step in creating a mobile application. It will help to define the direction and vision of the design and allow anticipation of future industry trends. Here are several questions to consider in this phase: What are the strategic priorities of the organization that are prompting this development? How will the application align with the business goals? And, most important, what is the problem to be resolved or alleviated with the design? For example, the organization may not have a mobile application for its customers to make purchases, inquire about returns, and other general needs. Creating a mobile application may increase customer satisfaction and generate exposure to the business, ultimately expanding the customer base. The development process should seek to create positive experiences for its targeted users through its functionality. Create a detailed plan that outlines the "why" to include an analysis of the problem, the overall goals, and how the design will ultimately align with the organizational strategic goals, including data to support the plan.
- User interface and user experience: These two elements work together within an application and should

be part of design consideration. The **user interface (UI)** is the point of interaction between the user and the product. Designing with UI in mind involves considering elements and functions that the user may encounter, and how the design responds to the user's needs. The **user experience (UE or UX)** is a design approach that integrates the user's experience with the company, its services, and its products. UE looks at the application design process from all aspects of a customer's interactions with a company's services. This process requires a keen understanding of the user, their needs, and their interactions with the application or system that is being designed. Much like the Agile approach, the UX approach keeps the user needs at the forefront of the development process.

- Application development, testing, and deployment: Taking into consideration the defined strategy and the plan to integrate the UI/UE approach within the design, begin developing the application. Leverage user stories, storyboards, and other visuals and mapping tools to outline the user's steps as they navigate the application. Does the design provide consistency? Are its core features available? Is the text legible? Is the navigation simple? Is it usable across platforms and with its web-enabled version (if available)? Does the design anticipate its user's needs, leading users to a positive end result and user experience? Review the design to validate that it meets the business and user requirements. Test the design to identify bugs or glitches that may impact its use, functionality, and performance (such as load times). Consider extending testing to a **focus group**, which is a group of individuals assembled to discuss their opinions on a product or service, as their insight could direct the future use of the product. Once the mobile design is validated, deploy the application and watch it in use.
- Application support and performance monitoring: Continue to monitor the mobile application via statistics and reporting methods to gauge its usability. Monitor user feedback and performance metrics, leveraging the resulting data to update future design iterations, if necessary.

CAREERS IN IS

Mobile Application Developer

A mobile application developer writes software programs for mobile applications across platforms, and they may be involved in the testing and future maintenance or updating of applications. These technical professionals work in a wide variety of industries. Other professionals who create similar, user-friendly software applications are software engineers, web designers, and iOS developers. A minimum of a bachelor's degree, industry certifications, and the completion of internships or entry-level work experience are generally expected to start .

Guidelines for Website Design and Usability

Have you ever visited a website and regretted it immediately? Why? Was the site hard to navigate, visually unappealing, or slow to load? Did you not find the information you were looking for? Examples of poor usability include a landing page that features several issues that contribute to an unprofessional look, such as too much information as text, uneven header and footer, and a lack of white space.

Certain common problems associated with web design often lead websites to their demise if not corrected. Unfortunately, many website owners do not even realize that their sites have these problems. Although these guidelines are not all universally applicable, following them can help web development teams to make sure websites are user friendly:

- Follow web content accessibility guidelines: The term **accessibility** refers to the practice of making products, services, and environments usable by as many people as possible, especially by ensuring that digital resources are available to individuals with disabilities. W3C is a Web Accessibility Initiative organization that maintains guidelines, strategies, standards, and resources for web design. It continues to expand its **web content accessibility guidelines (WCAG)** to incorporate accessibility guidelines for

organizations and individuals around the world. These international standards focus on a variety of information and content located on websites, from code to the presentation of the resulting text, images, and sound.
- Maintain common design elements: Design elements should be functionally minimal. Content should be clear and legible, and related ideas should be located in close proximity to each other and organized, through hierarchies, into common categories. Images, text, and sound elements should meet accessibility standards.
- Simplify navigation: A good website is easy to navigate and users are able to locate items quickly when they land on the site. Search or lookup features should be readily available and functional, and they should return targeted results based on the search input.
- Optimize for mobile devices: Most users now access websites via their mobile device. The use of a **responsive design** will allow the website's design themes and associated content to adjust to match and reconfigure themselves for mobile use.

A strong design features accessible font styles and colors along with being easy to navigate. The font is clear, well organized, and visually appealing. Good website design uses images, text, and sound elements that are within accessibility standards.

FUTURE TECHNOLOGY

Low Code and No Code

Low Code and No Code are two future technologies of mobile design that allow users with little to no programming or software development experience to build applications for business use. Drag-and-drop features of computerized models with prebuilt coded instructions and functions can be used to create valuable business applications. These technologies generate value by replacing legacy systems, providing interoperability options, being easy to use, and offering reduced development time compared with traditional development.

Key Terms

accessibility practice of making products, services, and environments usable by as many people as possible, especially by ensuring that digital resources are available to individuals with disabilities

Agile approach of iterative and incremental delivery of quality products and value to stakeholders using team collaboration, flexibility, and continuous planning

Agile software development adaptive approach to software development that considers uncertainty in rapidly changing environments and allows Agile teams to respond to those changes to deliver smaller, consumable work packages quickly

As-Is/To-Be process map visualization that details the “current state” and “future state,” respectively, of a specific process or function within an information system; the As-Is process map details how things currently work, while the To-Be process map describes what should be done to reach the desired future state

business problem any obstacle to business operations that causes variance in the expected outcome

client/server architecture tiered architecture in which a central computer (server) operates the network and allocates resources to the equipment connected to the network

computer-aided design (CAD) design approach in which computers are used to assist in the design process, including in the creation, development, modification, or optimization of design systems

context diagram high-level diagram that visualizes a system or parts of a system and the environmental actors with which it interacts using diagrammatic arrows to display the flow of data

data cycle different stages that data pass through while they exist in an organization’s system, from initial generation onward

data design aspect of systems design wherein data and the actionable components resulting from the systems analysis process are translated from their raw formats and combined into understandable formats

data dictionary database that houses the details of system data, their properties, entity relationships, and any reference documentation

data flow diagram (DFD) graphical representation of the information flow of a process or system

design diagram simplistic drawing, or elaborate depiction, that helps design teams as it is simple to understand, universally accepted, and easy to compare

enterprise another term for a business, organization, or company

enterprise network architecture includes pertinent business functions and provides and illustrates the technical architecture, including the dependencies and connectivity of various applications

entity relationship diagram (ERD) visual representation of the data flow and its relationship among people, objects, events, places, or concepts

flowchart visualization that displays sequential relationships between data, systems, programs, or processes and is often used by technical and nontechnical persons to document, plan, and communicate ideas in a simple-to-understand visual format

focus group group of individuals assembled to discuss their opinions on a product or service

functional requirement feature or function of an application that is needed for the affected business areas to accomplish its tasks

interface design design of the visual layout and functional elements of a product or system that involves using an understanding of people and processes to drive the final design outcomes

iterative process that is applied repeatedly

mind map free-form depiction of ideas with branches displaying the flow of information and thoughts; generally used for brainstorming activities

network system of interconnected computers and other devices that allow for the exchange of data and information (such as files) and the sharing of resources (such as printers)

network architecture top-level view of the system that defines the equipment in the network and the interaction between the equipment

network design focuses on the specific implementation and configuration of a network to meet the requirements of a particular organization or application

network protocol set of rules and guidelines that determines how data are exchanged between network devices

nonfunctional requirement attribute of the system that enhances its functionality or operation and is often viewed as an item that describes the general properties of the system or how the system should behave and work

peer-to-peer (P2P) architecture architecture in which computers on the network are all given the same opportunity to use resources on the network

process design activity generally used by businesses to further understand its processes and how to improve them

prototype design approach wherein systems designers and users create a small-scale representation or working model of the solution

requirements traceability matrix (RTM) spreadsheet or similar document used to record each user requirement along with supplemental information (such as type, description, objective, justification, priority, department, and status) that assists with the review, testing, and confirmation of requirements

responsive design approach that allows design themes and associated content to adjust to match and reconfigure itself for mobile use

retrospective meeting meeting in the Agile software development process at which sprints are discussed in detail and areas of improvement to apply to future sprints are identified

software development life cycle (SDLC) framework that defines the stages of software development, from inception to retirement

sprint time-based period, generally between one and six weeks, that represents a delivery cycle during which the specified work is completed and reviewed

stakeholder individual or group who has a vested interest or concern of a business decision; may be internal or external to an organization and may include the community, government entities, employees, customers, investors, suppliers, or trade unions/associations

stand-up ten- to thirty-minute daily meeting to discuss the development process and any changes that are needed during sprints

system design process methodology that determines and defines the architecture, interfaces, and data for a system to ensure that it satisfies the specified requirements

system documentation reference information used to describe the system and its parts and used to understand the functioning of the system

systems analysis identifies the opportunities discovered by examining business problems and identifying possible solutions the business may undertake

systems analyst professional whose primary functions are to utilize systems analysis and design techniques to support information systems and solve challenges that arise when using information systems

systems design organizational approach to improving on an existing system or to developing a newer one

systems design task list road map through each step of the design process, allowing teams to have an organized workflow and make informed decisions at each step

UML diagram broad category of tools that are commonly used in systems analysis and design

usability quality-related attribute that assesses an interface's ease of use

use case diagram visual representation of system features that displays how specific users interact with the specific functions of a system

user experience (UE or UX) design approach that encompasses the user's experience with the company, its services, and its products

user interface (UI) point of user interaction with the product that incorporates the elements, functions, and responsiveness of the design that the user may encounter

user requirements aspects of a solution that are specified by stakeholders and needed to support the specific needs and expectations of a business process or product

user-centered design (UCD) iterative, and stepwise, approach to development that considers the user's needs, behaviors, and preferences

web content accessibility guidelines (WCAG) guidelines for web and digital design that integrate accessibility into the product and user experience

Summary

4.1 Systems Analysis and Design for Application Development

- Systems analysis and design is a stepwise process for evaluating and developing information systems by understanding the needs of the business to improve on or develop effective and efficient functioning solutions to technical challenges.
- The benefits of systems analysis and design include the identification of operational efficiencies achieved by improvements to existing systems, the alignment of system functionality with organizational strategic objectives, early risk identification of potential threats to processes, the minimization or reduction of resources and costs, and the overall improved quality, efficiency, productivity, and usability of the system.
- A systems analyst is a professional whose primary functions are to utilize systems analysis and design techniques to support information systems and solve challenges presented when using information systems.
- Systems design generally involves the following activities: designing the data, interface design, and process design. The tools used in systems analysis and design are varied and aid in the understanding of the system in its current and/or future state.
- SDLC is a framework that defines the stages of software development, from its inception to its retirement, providing a blueprint of the tasks to be completed for each stage of the cycle: analysis, design, development, testing, deployment, and maintenance.
- Agile is an iterative approach to software development that considers uncertainty in changing environments and allows Agile teams to respond to those changes quickly to deliver smaller, consumable work packages. The Manifesto for Agile Software Development maintains the four Agile Manifesto values and describes how Agile development works, including the planning and preparation involved and the importance of sprint planning.
- An analysis and design team includes members such as the designer, systems architect, user experience researcher, and systems analyst, among other important participants in the systems analysis and design process.

4.2 Defining the Business Problem and User Requirements

- Defining the business problem is multifaceted and includes asking directed questions to uncover the issues that need to be addressed and the problem at hand.
- Various tools can be used to understand user needs and how users will interact with the system. These include both visual tools, such as flowcharts, and textual tools, such as user stories.
- Not having complete or correct user requirements can delay a project and result in additional costs. Taking time up front will save valuable resources in the long run.
- Through proper planning in the early stages of systems development, analysts can feel confident in delivering a system that works for the stakeholders and meets the user requirements.

4.3 Technical Design Methodologies and Practical Applications

- The systems design process defines the architecture, interfaces, and data for a system that satisfies the specified requirements.
- Systems designs can be logical (a high-level view of the system, including actors and the relationships between the actors and the system) or physical (the specific hardware and software components, along with detailed systems diagrams and layout of the systems).
- Data move through the system in a cycle from initial data creation to the eventual archiving or destruction of the data.

- Prototypes are used for early detection of problems, expanded user engagement, increased satisfaction with the final product, and greater savings of time and money associated with rework. CAD is used by designers and engineers because of its ease of visualization, level of detail, capacity for specialization, and ability to optimize products and render a physical product, which can greatly inform the design process.
- Input/output control is a component of the design process. Input is the raw data that are processed through the functions of the system. It is controlled by the directives used to submit responses into the system by the user, producing an output according to the system logic. Output is the information delivered to users through an information system; it is the data that result from the inputs being processed according to the system logic.
- A systems design task list provides a road map through each step of the design process, allowing teams to have an organized workflow and make informed decisions through each step.
- The enterprise network system is composed of interconnected computers and other devices that allow for the exchange of data and information and the sharing of resources.
- The most commonly used network architectures are peer-to-peer and client/server.

4.4 Designing for Mobile Devices and Other Design Considerations

- User-centered design (UCD) creates a product that uses an interdisciplinary approach to design with focus on the user experience and feedback. Applying user feedback to guide the design process strengthens the output of the design and creates a relationship with the user.
- UCD is iterative in nature and includes the practices of building, refining, and improving a product, project, or initiative.
- Best practices associated with a UCD approach include defining the business goals, understanding users and aligning business goals, generating the design solution, evaluating the final product, and continuing to refine the product.
- Mobile applications require special design considerations. This includes keeping the flow simple, highlighting key features of the application, and designing features for touch screens.
- Effective website design includes making sure accessibility standards are met for images, text, and sound. The website design should also incorporate mobile accessibility in the process.

Review Questions

1. What is a drawback of systems analysis and design?
   a. delays early identification of potential threats to processes
   b. increases resources and general costs
   c. prevents the alignment of strategic objectives
   d. decreases quality, efficiency, productivity, and usability of the system

2. What is the tool used in systems analysis and design that documents the details of the design?
   a. simulation
   b. data flow diagram
   c. pseudocode
   d. data dictionary

3. What is a statement that best characterizes the Agile software development process?
   a. It is a linear approach to software development and proceeds sequentially from one stage to the next.
   b. There are no considerations for environmental changes.
   c. The final work product is delivered in one package at the end of the process.
   d. It values individuals and interactions over processes and tools.

4. What is a responsibility of the systems architect role?
   a. to conduct user testing to validate ideas
   b. to create the hardware, software, and network systems

c. to create and test software solutions
d. to detail the technical specifications of the system

5. A small start-up is developing a mobile app and has limited resources. The team wants to release a basic version of the app quickly, gather feedback, and make iterative improvements based on that feedback. The team also expects some changes to the app's features as they learn more about user needs. Given these conditions, which of the following best describes the most suitable approach for the team?
   a. Use a Waterfall approach to ensure all features are fully developed and tested before the first release, preventing any major changes after the launch.
   b. Follow an Agile development process to focus on delivering a minimum viable product (MVP), gather user feedback, and iterate on the app with each new release.
   c. Adopt a hybrid approach, combining elements of Agile and Waterfall, to maintain flexibility in development while still following a strict, sequential timeline.
   d. Use a Rapid Application Development (RAD) model to complete the app's features as quickly as possible, with minimal user involvement during the development process.

6. What is the purpose of the five-whys method?
   a. to determine solutions to the business problem or opportunity
   b. to evaluate the solution
   c. to evaluate the options presented
   d. to define the problem

7. What would indicate that an update or reassessment of the user requirements is needed?
   a. documented processes
   b. early delivery of the product
   c. meeting user functional requirements
   d. increased costs

8. Dr. Singh could benefit from having a systems analyst support her business problems and opportunities. How could Dr. Singh leverage this resource most efficiently?
   a. by focusing on opening the new practice location and not addressing challenges within the current practice
   b. by engaging all stakeholders in discussions with the systems analyst to gain a comprehensive understanding of the business problems and opportunities
   c. by fixing the problems in the current practice and delaying the opening of a new office
   d. by purchasing a system "off the shelf" and adjusting the business to fit the new system

9. What is an example that demonstrates the importance of clearly defining business problems and user requirements at the start of a systems development project?
   a. Focusing on user requirements can prevent misunderstandings during the development process but will not influence project costs or timeline.
   b. Incomplete or incorrect user requirements may lead to significant delays and increased costs, but addressing them in early stages helps avoid costly changes later.
   c. Analyzing user needs only at the final stages of development ensures that the system meets stakeholder expectations without wasting resources.
   d. Relying on visual tools, such as flowcharts, exclusively, will guarantee that user needs are fully understood and eliminate the risk of project delays.

10. When should the systems design process begin?
   a. before the business problem is defined, prior to completing a systems analysis, during the requirements gathering process, and prior to the generation of design diagrams
   b. after the business problem is defined, prior to completing a systems analysis, during the requirements gathering process, and after the generation of design diagrams

  - **c.** after the business problem is defined, after completing a systems analysis, after completion of the requirements gathering process, and after the generation of design diagrams
  - **d.** after the business problem is defined, prior to completing a systems analysis, during the requirements gathering process, and prior to the generation of design diagrams

11. What differentiates logical designs from physical designs?
  - **a.** Logical designs include the specific hardware that will be used in the system.
  - **b.** Physical designs incorporate business processes to visually represent the flow of data and the relationships between them.
  - **c.** Logical designs provide a high-level representation of the system.
  - **d.** Physical designs are used to build out the logical design.

12. Why are communications protocols part of the network?
  - **a.** They help diagnose connectivity issues.
  - **b.** They allow for the exchange of data and information.
  - **c.** They allow for the connectivity of most devices.
  - **d.** They ensure safe data transmission.

13. Which statement best illustrates the importance of the systems design process in ensuring a successful project outcome?
  - **a.** A systems design focuses primarily on choosing the right hardware to meet performance requirements, ensuring the system functions as expected.
  - **b.** The systems design process creates detailed architectural and data specifications, balancing logical and physical components, while also identifying potential issues early through prototypes and iterative design.
  - **c.** A systems design is only about developing the user interface, focusing primarily on aesthetics and ease of use.
  - **d.** The systems design process is mainly concerned with generating the necessary documentation and does not need to consider user feedback or future scalability.

14. What is a key goal of using a user-centered design approach?
  - **a.** providing the cheapest solution to the user in the quickest time frame
  - **b.** integrating customer feedback once during the development process
  - **c.** developing detailed documentation reports of the system functionality
  - **d.** utilizing user input throughout the process to provide the best solution to meet the needs of the users

15. Why is it important to conduct research before designing a mobile application?
  - **a.** Research helps create an app with the least amount of time and cost.
  - **b.** Research tells you how to design the product.
  - **c.** Research prevents costly mistakes and major changes later in the design process.
  - **d.** Research provides new revelations about user needs.

16. What is a consideration for mobile application design?
  - **a.** trendiness in design
  - **b.** predetermined response time
  - **c.** finger-friendly navigation
  - **d.** complex but functional design

17. What is a true statement about UI and UE?
  - **a.** UI and UE work independently of each other.
  - **b.** There is minimal difference between UI and UE.
  - **c.** UE considers the interaction of the user with the design.
  - **d.** UI looks at the design process, encompassing the user's experience with all aspects of the company's

services.

18. Which statement best describes the role of iterative design and user feedback in a user-centered design (UCD) approach for product creation?
    a. Iterative design ensures that the product is perfect from the start, avoiding the need for user feedback after the initial launch.
    b. User feedback in UCD is only relevant during the initial concept phase, and iteration focuses solely on technical performance.
    c. UCD uses continuous user feedback to guide iterative improvements, creating a product that aligns closely with user needs and business goals.
    d. Iterative design in UCD is focused primarily on aesthetic improvements, deprioritizing functionality and accessibility requirements.

Check Your Understanding Questions

1. Describe the concept of systems analysis and design.
2. Explain the SDLC process in your own words.
3. Identify methodologies and tools in systems analysis.
4. What would be your preferred tool to use to complete a systems analysis and why?
5. What importance does each of the roles and responsibilities ascribed to the analysis and design team have?
6. Why is it important for businesses to solve business problems? Explain.
7. Explain the purpose of a requirements traceability matrix (RTM).
8. If you had to create a design diagram to communicate two different solutions to Dr. Singh for her problem/opportunity, which design diagram would you use and why?
9. What might be some of the challenges associated with the requirements gathering process?
10. What are the aspects of a good systems design?
11. What are the fundamental differences between logical and physical designs?
12. What are some pros and cons of creating a prototype?
13. Why is it important that the enterprise network architecture be considered in developing and designing an application?
14. Why is user-centered design important?
15. When should strategic development and planning occur in the mobile application development process, and what is the importance of this step?
16. Would you consider UI or UE more important? Explain how you would prioritize features of a website design.
17. Explain how globalization affects mobile application design.

Application Questions

1. Reflect on the Agile methodology and the characteristics of Agile teams:
    a. How might the Agile approach be applied to a team project for a class you are in that lasts the duration of the term and has a final presentation and paper due the last week of the term?
    b. What is your ideal time period for a sprint for a semester-long team project that you are assigned and

why?
c. What tools would you use to maintain engagement in the project?

2. In a small group or on your own, reflect on a business problem in your current organization (work or school).
   a. Identify an opportunity for improvement in your organization’s function or operation.
   b. Who would you enlist to assist with requirements gathering?
   c. What tools will you use to assist your efforts?
   d. What are some other factors you should consider?

3. Discuss the inputs and outputs that could be present in Dr. Singh’s system. Include how the data move through the data cycle in the system.

4. Reflect on a website or a mobile application that you frequently use or visit.
   a. Discuss what you like and dislike about the website or mobile application. How would you describe its usability?
   b. If you have any dislikes, why do you continue to visit this website? Are there competitor websites, and how do they differ?
   c. Does the website or mobile application allow you to submit user feedback? If so, have you ever submitted feedback on the website’s usability? Why or why not?

5

Information Systems Security Risk Management

Figure 5.1 Protection from cybersecurity attacks works in a similar way to how we protect ourselves from bad weather—by using different layers to shield us from the elements. (credit: modification of work "Clear Umbrella Rain Liverpool" by Freddie Marriage/ Wikimedia Commons, CC0 1.0)

Chapter Outline

Introduction

Imagine carrying important documents, such as a paycheck or a diploma, when it starts to rain. Without an umbrella, your documents can be damaged, although it may be possible to reprint them. However, if the rain turned into a violent storm, you'd need much more protection to keep your documents safe. Similarly, in information technology, our digital lives are constantly threatened by malicious actors, rogue governments, and natural disasters.

Just as an umbrella alone isn't enough to protect someone from a storm, people rely on multiple layers of protection to shield their digital lives. As a person navigates the digital landscape, layers of security help keep them safe, preventing severe damage that's much harder to remediate.

5.1 The Importance of Network Security

Learning Objectives

By the end of this section, you will be able to:

- Determine the difference between information security and information privacy on a public or private network
- Define the key principles and concepts of network security and their importance
- Describe potential network vulnerabilities and threats

Network security is dynamic, requiring ongoing adjustments to counter rising vulnerabilities and threats. What may be considered safe today may not be in the future. The ever-changing nature of this field necessitates a comprehensive understanding of various technologies and advancements that influence security. The implications of a network security breach can be diverse, ranging from minor disruptions in operations, to severe data loss or compromise. Therefore, understanding the significance of network security can contribute to a larger societal benefit. It is important for IS professionals to have a conceptual understanding of network security, its mechanics, and why this protection is a key aspect of modern life, as well as the practical skills needed in securing a network.

Information Security and Information Privacy on a Public or Private Network

In the field of **cybersecurity**—which is the practice of protecting systems, networks, devices, and data from online threats—information security and information privacy are not identical terms, although they are related. On one hand, **information security** is the practice of protecting information by mitigating information risks and vulnerabilities, which encompasses data privacy, data confidentiality, data integrity, and data availability and employs methods such as encryption, firewalls, and secure network design. Its aim is to shield both organizational and individual data from unauthorized access or tampering. In contrast, **information privacy** involves the right and measure of control individuals have over the collection, storage, management, and dissemination of personal information. Information privacy involves policies regarding what data are collected, how they are stored, and who has access to share information.

The two domains of information privacy and information security are not static; they are influenced by technological advancements and emerging threats. This makes continuous learning and adaptation important for anyone interested in the field. Both students and seasoned professionals need to maintain their skills and understanding to keep up with advancements in the field. This may include learning about the latest encryption methods or understanding new data privacy laws that impact the organization.

Although both information security and information privacy are equally important, they tackle different aspects of data protection. Think of information security as a bouncer at a club. Its job is to keep unwanted guests out, so it uses tools such as encryption to hide the important data, firewalls to block unauthorized entry, and secure networks to chase away any intruders. Information privacy, then, is more like getting access to the VIP room inside that club. It manages who gets in, who sees what, and what goes on inside. Imagine you have a list of the criteria for who can access the VIP room. When you're not updating it, you keep it locked in a special drawer that only you have the key to, thus keeping the contents private. But privacy also includes making sure unauthorized people do not know who is on that list, or even that it exists.

In short, information security is about guarding the perimeter and protecting your assets, while information privacy is about managing access and keeping sensitive data private. Both are essential, but they play different roles in keeping your digital world safe. At the core of both information security and information privacy is a foundational model in cybersecurity that ensures information is protected and readily available to authorized users, called the **confidentiality, integrity, and availability (CIA) triad** (Figure 5.2).

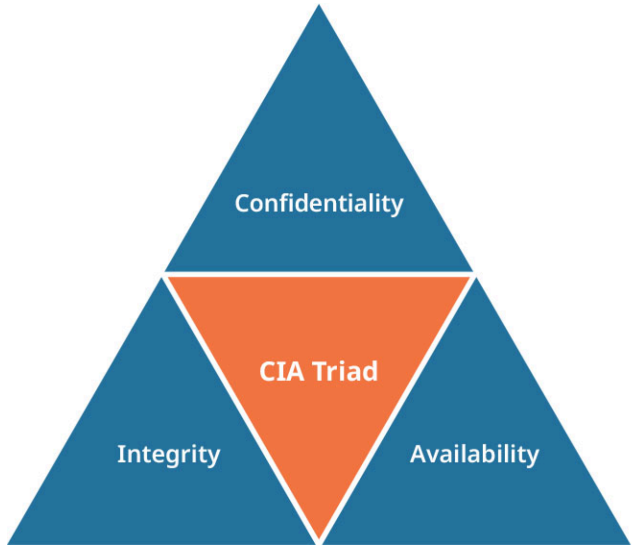


Figure 5.2 The confidentiality, integrity, and availability (CIA) triad is the cornerstone framework for information security that aids in promoting the security and reliability of information systems. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The CIA triad is the backbone for creating cybersecurity systems, aiming to strike a balance between keeping things secure and ensuring that the people who are authorized to access the data and systems have access to it. As the name implies, the CIA triad is divided into three domains:

1. The measures that are meant to prevent sensitive information from being accessed by bad actors or by those users who have not been granted access is called confidentiality. The intent is to keep data in the correct hands and away from those who want to cause harm or exploit information for nefarious purposes. Additionally, confidentiality addresses policies involving human error, such as users not keeping strong passwords, failing to secure sensitive information when not in use, and falling prey to scammers. Scams often involve **phishing**, which is a type of social engineering attack that appears as a trustworthy entity in digital communication but steals user data, such as login credentials and financial information. Two means of applying confidentiality to an IT system are encryption and access controls.
2. Preserving the fidelity of data over its life cycle is called integrity. Any alteration to database tables, user records, or other data can be very damaging, often causing legal ramifications or loss of operations. Two means of maintaining the integrity of data are hashing and digital signatures.
    - The process of converting data into a fixed-size string of characters, typically used for security purposes to ensure data integrity, is called **hashing**. Hashing can verify the authenticity of a file by assigning a hash algorithm, such as Secure Hashing Algorithm 256 (SHA-256) that has a 64-character hexadecimal hash value assigned to the file by the algorithm. This results in a hash of characters that represent every point of data in the file, bit by bit. Even the smallest change in the file results in a drastically different chain of characters.
    - An electronic signature that uses cryptographic techniques to provide authentication and ensure the integrity of the signed digital document or message is a **digital signature**. They are used in online documents such as emails, bank documents, and online forms, and employ the public key infrastructure (PKI) to protect the confidentiality and integrity of data during transit. This method works by supplying a public and private key to each user transmitting information. Aside from protecting the confidentiality and integrity of data during transit, this framework helps to verify the authenticity of a file and its sender.
3. Ensuring that authorized users can access resources such as networks, databases, and other systems is called availability. This part of the triad often encompasses disaster recovery and response plans. There are several ways to maintain availability, such as keeping up with upgrades on equipment and software, maintaining backups in case of an attack or system failure, and ensuring that redundant systems are in

place to protect the IT system.

Think about the CIA triad like this: Imagine you have a personal diary, and you want to make sure nobody else can read it. When you're writing in it, you want to be able to access it easily, but when you put it away, you want to feel confident that no one else can access it.

Storing your diary in a safe when you're not using it is a way of keeping it confidential. You could also put a seal on it, so if someone does try to tamper with it, you'll know; that's maintaining its integrity. Keeping the safe somewhere close, so you can get to your diary whenever you need it ensures that it is always available to you. This way, you've covered all the bases of the CIA triad.

Information Security

When we think of data, most of us envision pictures, documents, and videos. However, data come in all sorts of formats, types, and sizes. While our media is an important piece of the data puzzle, other types are equally important. Consider the security of passwords, bank account information, employee records, and text messages. These types of data also require both information security and information privacy. For example, in a workplace setting, protecting employee information involves encrypting sensitive data (information security) and implementing privacy policies to regulate who can view or modify this data (information privacy).

Moreover, the landscape of data protection is becoming increasingly complex with the rise of generative AI. Most organizations use generative AI, but only a third of them implement protection from generative AI threats because most companies do not fully understand the dangers. Currently, generative AI benefits attackers more than organizations, but that may change in the near future.[1] This intersection of advanced technology with traditional data types underscores the critical need for robust security measures. Acknowledging opportunities and threats posed by generative AI, blockchain, and other emerging technologies can help in developing more effective strategies to safeguard all forms of data.

Intellectual Property

Creations of the mind that are protected by law from unauthorized use or replication are called **intellectual property (IP)**. It can include inventions, literary and artistic works, designs, symbols, names, and images used in commerce. IP is often a target for cybercriminals and nation-state threat actors looking to steal technology for their own benefit. Imagine dedicating years of research and millions of dollars to an expensive project only to lose the information to a hacker in minutes. Unfortunately, hackers may still be able to bypass security controls to access an organization's IP.

Financial Data

Financial data are considered sensitive information, which is data that require high levels of confidentiality and security. Sensitive data can include financial data related to transactions and personal finance details, and employee data involving personal and professional details. Protecting this information is crucial to helping organizations prevent fraud, maintain stakeholder trust, and comply with governmental regulations. Security measures used to protect financial data often use a layered approach beyond firewalls and encryption that combines multiple security barriers and includes rigorous auditing and multi factor authentication.

Employee Data

Personally identifiable information, such as Social Security numbers and addresses, constitutes an entity such as employee, customer, or student data. Although they may not seem very sensitive, these data are valuable to hackers for identity theft, corporate espionage, harassment, and extortion. Organizations must use measures such as encryption and the principle of least privilege to protect this information.

1 Jim Tyson, "Only One-Third of Firms Deploy Safeguards Against Generative AI Threats, Report Finds," Cybersecurity Dive, May 13, 2024, https://www.cybersecuritydive.com/news/generative-ai-safeguards-splunk/715897/

Network Configurations

Network configurations are the physical and logical elements that form a network, such as servers, routers, switches, and software. A **server** is a powerful computer or computer program that provides data to other computers (clients) over a network. A **router** is a device that forwards data packets to the appropriate parts of a computer network. A **switch** is a device that connects and segments various components within a local network. Access to these systems by bad actors or rogue employees can have dire consequences for an organization. Unauthorized access to network configuration data could allow an attacker to map out a network, identify weaknesses, and access private customer information.

Internet protocol addresses, along with media access control addresses, are essential elements of a network that require protection. An **internet protocol (IP) address** is a unique identifier that allows a computer to be addressed in order to communicate on the internet. A **media access control (MAC) address** is a unique identifier that allows a computer to be addressed in order to communicate within a local area network. To gain unauthorized access to a network, attackers often use a technique called port scanning for penetration or determining an entry point. These scans allow an attacker to gather information about a network such as the unique addresses of each of the components connected. With this information, hackers can spoof addresses, which allows them to blend into the network undetected. To protect IP addresses and equipment identifiers, organizations use VPNs or proxy servers to mask IP addresses and create a secure tunnel for employees accessing information from remote locations. Passwords account for the largest vulnerability to a network due to the human factor involved. According to *Security Magazine*, close to 75 percent of users are at risk for compromise due to weak password practices.[2] Additionally, it is also estimated that nearly 80 percent of data breaches are caused by poor password management. To prevent attacks due to poor password practices, organizational leaders should implement the policies shown in Table 5.1.

Password Policy	Description
Password standards	Implement password length standards (at least eight characters) and encourage the use of complex passphrases.
Password expiration	Impose periodic password expiration dates, requiring employees to change their passwords semiyearly or annually.
Multi factor authentication	Use multi factor authentication to add another layer of protection by requiring an additional form of authentication, such as an access code.
Password policies	Ban common passwords that can be easily used by attackers.

Table 5.1 Good Password Practices Best practices in securing data keep information safe from attackers.[3]

Information Privacy

Information privacy is a critical aspect of cybersecurity and encompasses the practices, policies, and regulations that are designed to protect people and systems from unauthorized access and harm. This includes protection from access to personally identifiable information (PII), health-care records, financial statements, and data from devices such as smartphones, smartwatches, and other wearable tech.

2 Security Staff, "3 in 4 People at Risk of Being Hacked Due to Poor Password Practices," *Security*, June 21, 2023, https://www.securitymagazine.com/articles/99529-3-in-4-people-at-risk-of-being-hacked-due-to-poor-password-practices
3 "Password policy recommendations for Microsoft 365 passwords," Microsoft, last modified May 28, 2024, https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

Understanding the principles behind establishing and preserving information privacy is key to ensuring that data remains safeguarded while in transit and at rest.

Additionally, the concept of information privacy is based on a variety of policies and regulations that guide leaders and managers on how to safeguard sensitive information. As the scope of data needing protection continually expands, improvements are constantly being made to address the complexities of new, emerging technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence.

In addition, different sectors have their own specific frameworks and laws. In the United States, institutions such as hospitals or those who deal with sensitive medical information must adhere to the guidelines outlined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In the education sector, educational institutions must adhere to the principles outlined in the Family Educational Rights and Privacy Act (FERPA).

HIPAA

Established in 1996, HIPAA was introduced by the Health and Human Services Department (HHS) to devise legislation that would protect the privacy of those seeking medical care. One part of HIPAA, the Privacy Rule, sets standards and guidelines for organizations that manage patient information and medical records of any kind. This includes health plans, health-care providers, health-care clearinghouses, and business associates.

HIPAA provides rigorous standards for companies that possess and interact with a vast range of protected health information (PHI), such as medical history, billing information, and patient identifiers. Moreover, HIPAA's controls do not apply solely to medical providers, but rather to any entity that may possess or have access to patient data. This includes third parties who provide data hosting services, accounting firms, consultants, or any entity contracted to maintain hosting services such as patient portals and websites.

In addition to the Privacy Rule, HIPAA has a Security Rule, which works with the Privacy Rule to lay out the technical, administrative, and physical measures needed to protect electronic health information, thus tying into the larger world of information security protocols. Failure to comply with HIPAA can result in significant penalties, ranging from fines to criminal charges. These enforcement actions remind organizations to thoroughly adhere to the established guidelines and to continually update their practices.

FERPA

FERPA is a U.S. federal law that was enacted in 1974. Its main goal is to give parents and students who are 18 years and older some control over their educational records. Specifically, FERPA sets rules on who can access these records and under what circumstances. Educational institutions that receive federal funding are required to comply with FERPA's mandates, and noncompliance could result in the loss of that funding.

FERPA gives students and their parents the right to access their educational records, correct any mistakes, and have a say in how that information is shared. While this sounds simple, the implementation can be complex. For example, schools must have written consent to release information, but there are exceptions such as cases involving subpoenas or emergencies. It is important to note that not all information is protected under FERPA. Some types of directory information, such as a student's name, address, and telephone number, can be released without explicit consent, unless the student or parent opts out.[4]

To understand how FERPA protects academic information, consider a student attending a college away from home whose parents demand to know their student's test scores, homework assignments, and regular activity in classes. Under FERPA guidelines, if the student is 18 years old or older, the only one who can release that information to the parents is the student. Their parents would have no access to this type of information from the school without the student's explicit permission, except in health or safety emergencies.

4 U.S. Department of Education, "FERPA: 34 CFR PART 99 --Family Educational Rights and Privacy," accessed January 31, 2025, https://studentprivacy.ed.gov/ferpa

Key Principles and Concepts of Network Security

In the complex world of cybersecurity, it is important for everyone to understand the foundational principles of the threats to digital security and the ways to safeguard digital assets. Whether you are a student, a new employee, or a boardroom executive, having a firm grasp on the key principles can help protect you from digital harm.

Imagine you're setting up a home network. You notice that your devices receive different IP addresses from time to time. This is because many IP addresses are dynamic, changing with each connection. Now, visualize managing a large corporate network where stability and reliability are critical. Here, a company can use a **static IP address**, which is a permanent address assigned by an administrator that remains the same over time and is essential for services such as hosting servers, email servers, and network devices, or when remote access is required.

The consistency of a static IP address allows for reliable and straightforward network management, as well as easier implementation of security measures because the address can be precisely identified and controlled. Static IP addresses are used primarily for servers and network equipment. A **dynamic IP address** is one that is assigned each time a device connects to the internet and changes periodically, although not necessarily every time the device connects. This type of IP addressing is commonly used in residential and small business settings, where internet service providers (ISPs) assign these addresses to customers, and in larger companies for their client machines. Dynamic IP addressing is highly efficient for ISPs as it allows for the reuse and reallocation of a limited pool of IP addresses, optimizing the use of the IP address space, especially given the vast number of devices connecting and disconnecting from the internet.

The Internet Protocol version 4 (IPv4) is the fourth version of the fundamental protocol used for identifying devices on a network and routing data between them over the internet. It consists of four 8-bit groups that make up 32 bits total. In any given IP address under the IPv4 system, the range cannot exceed 256 in any 8-bit group; however, due to system limitations, addresses normally range from 0 to 255. The Internet Protocol version 6 (IPv6) has eight hexadecimal groups that allow up to 128 bits. There are many differences between these standards. For example, IPv6 can supply more security and a nearly limitless number of IP addresses (7.9×10^{28}). IPv6 is more secure than IPv4 because it was designed with built-in support for **Internet Protocol Security (IPsec)**, which is a suite of protocols that provides end-to-end encryption and secure data exchange. Additionally, its massive address space allows for more efficient address allocation, reducing the risks of IP conflicts and improving overall network reliability.

Both IPv4 and IPv6 addresses often come accompanied by a **subnet mask**, which is an address used in routing and network organization that divides the IP address into network and host addresses. One method for allocating IP addresses is **classless inter-domain routing (CIDR)**, which routes IP packets more efficiently than traditional classful IP addressing. CIDR is a key element of the IPv4 addressing method, as it increases efficiency and security by permitting the "borrowing" of bits of information to create a new range of IP addresses to form a **subnet**, which is a logically visible subdivision of an IP network. The subnet mask and CIDR help in segregating the network portion of an IP address from the host portion. This segregation is important for routing and for defining network boundaries, as it permits for the proper distribution of information and traffic to the intended recipient.

Another vital aspect of IP addressing is the way these addresses are allocated and managed. IPv4 addresses were developed in 1981 and were initially distributed in an erratic manner, leading to inefficient use of the address space. In contrast, IPv6 addresses are allocated based on a more hierarchical and organized structure, allowing for easier management and better security protocols. This process is managed by several organizations globally, such as the Internet Assigned Numbers Authority (IANA) and the five Regional Internet Registries (RIRs), ensuring a standardized approach to address allocation.

The **Domain Name System (DNS)** translates human-readable domain names to IP addresses, allowing users to access websites using familiar names. Essentially, it acts like a directory of the internet. This process is fundamental to web navigation, as it makes it possible for people to access information online without needing to remember complex numeric addresses. Just like a contact list keeps numbers, a DNS keeps IP addresses. Also, just like a contact list, these numbers must be updated frequently as people and equipment change. Figure 5.3 depicts how a DNS matches the client's computer (i.e., IP address) to an organization's website. While DNS is integral to web navigation, it can be exploited for malicious purposes, such as DNS spoofing, an attack where hackers corrupt DNS servers to redirect traffic to another server or website.

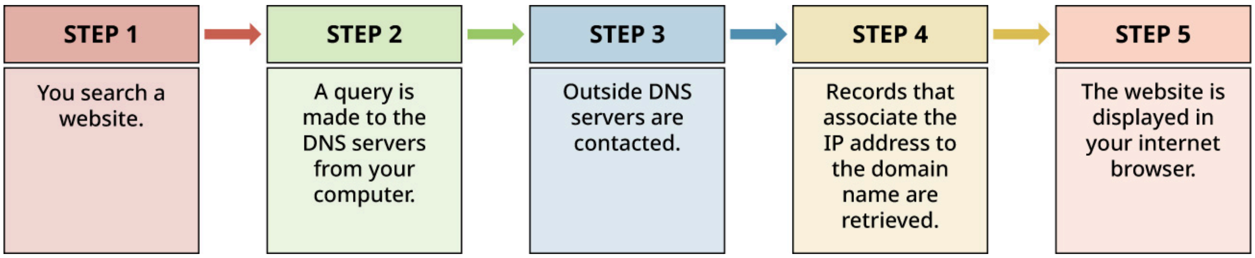


Figure 5.3 A DNS helps to identify and align the correct IP address to the URL. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

It is crucial to implement DNS security measures to mitigate vulnerabilities. One way is to use Domain Name System Security Extensions (DNSSEC), a suite of extensions that add security by enabling DNS responses to be digitally signed and verified. This verification process helps in safeguarding against DNS spoofing and other types of DNS-based attacks. Furthermore, securing DNS resolvers with threat intelligence that prevents users from accidentally visiting sites that could compromise their security can also help block known malicious domains. Implementing these advanced DNS security measures is increasingly considered best practice in both professional and consumer settings. One type of threat DNSSECs can prevent is those involving DNS spoofing, such as a man-in-the-middle (MitM) attack, which is one that manipulates the DNS to redirect a website's traffic to a different IP address, often controlled by the attacker. This allows the attacker to intercept and potentially modify the communication between the user and the intended website.

Another fundamental concept in network and information security is **encryption**, which transforms legible data into a coded format, making it unreadable to unauthorized entities. The encrypted data can only be converted back into its original format, a process called decryption, with the proper **cryptographic key**, which is a string of data used by encryption algorithms to encrypt and decrypt data. Encryption is particularly effective for safeguarding sensitive information during transmission or storage, making it an important tool for protecting data privacy and integrity.

The two most common types of encryption are symmetric and asymmetric. With **symmetric encryption**, the same key encrypts and decrypts the data. This approach can quickly and easily handle a lot of data all at once. The tricky part, though, is that both parties need to have the key, and sharing it securely can be challenging. In **asymmetric encryption**, also known as public-key cryptography, a public and a private key secure the connection. This eliminates the need to securely share a key, but it is slower than symmetric encryption. Each type of encryption serves specific use cases: symmetric is often used for data at rest, and asymmetric for data in transit. Asymmetric encryption is used in **Secure Sockets Layer (SSL)**, a communication protocol that establishes a secure connection between devices or applications on a network by encrypting data sent between a browser and a website or between two servers, and **Transport Layer Security (TLS)**, an updated version of SSL that uses an encrypted tunnel to protect data sent between a browser, a website, and the website's server. TLS prevents unauthorized access to messages and protects against hackers hijacking connections. The standard symmetric encryption algorithm used globally to secure data, known for its speed and security, is **advanced encryption standard (AES)**, while **RSA encryption** is a commonly used asymmetric cryptographic algorithm used for secure data transmission that is particularly useful in public-key cryptography.

The mechanism of **authentication** is the process of verifying the identity of a user, application, or device trying to access a network or system, often through credentials such as passwords or digital certificates. This can range from simple methods such as username and password combinations to more sophisticated techniques involving **multi factor authentication (MFA)**, which is a security measure that requires users to verify their identity using multiple forms of credentials, such as a password, a security token, or biometric data, to access a system. MFA might require something you know (password), something you have (a mobile device for a token), and something you are (biometrics such as a fingerprint). Proper authentication methods are vital to ensuring that only authorized personnel have access to sensitive data and systems. However, if mismanaged, they could also become a massive security risk, such as if someone gained access to your biometric data to imitate your likeness.

Other key components in network security include firewalls, intrusion detection systems (IDSs), and virtual private networks. A **virtual private network (VPN)** is a service that creates a secure, encrypted connection over a less secure network, typically the internet, ensuring private data remains protected. A **firewall** is a network security system that uses security rules to monitor and control incoming and outgoing traffic, typically between a trusted network and an untrusted entity (such as local area networks or the internet). Intrusion detection systems (IDSs) are more advanced in their capability, as they use pattern detection. Firewalls are mostly a preventive measure, whereas IDSs are a detective measure. IDSs can watch network traffic to detect anomalies that could be a security breach. VPNs, on the other hand, are network configurations that can supply a secure virtual tunnel for data transmission, often used for establishing secure remote access to a network. Think of a VPN as a private, secure, virtual tunnel through the internet. This tube ensures that no one can intercept or access the data during its journey. Similarly, a VPN encrypts your internet connection, creating a secure tunnel that protects your data from hackers, spies, and other potential threats, ensuring that your online activities remain private and secure. Together, these technologies form the foundational layers of a comprehensive network security architecture, each serving a specific role but collectively contributing to the robustness of the entire system.

Network Vulnerabilities and Threats

Network vulnerabilities and threats are critical issues that impact the security posture of any organization. Weak configurations, outdated software, and lax security policies often make networks susceptible to a range of malicious activities. Understanding these vulnerabilities is a fundamental step in fortifying a network's defenses.

Types of Network Vulnerabilities

When it comes to network security, software vulnerabilities often serve as an open door for attackers. A software vulnerability is a weakness or flaw within a software system, particularly in outdated or unpatched systems, that can be exploited by cybercriminals to gain unauthorized access or to disrupt the software's normal functioning. Outdated software and unpatched systems are particularly risky because they may have known flaws that have not been addressed, making them a target for cybercriminals. Imagine your software as a building: If everyone knows there is a broken lock on one of the doors, it is only a matter of time before an unauthorized individual enters. Therefore, keeping software up to date is essential.

Several new vulnerabilities have been introduced into the digital world with the advent of **artificial intelligence (AI)**, the branch of computer science focused on creating intelligent machines capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. One beneficial use of AI is to generate complex passwords. However, the technology can also be used in damaging ways. For example, computer-generated voices have increased robocalls, causing excess cell network traffic, and have been used by attackers to exploit and steal money from victims in social engineering attacks. Attackers have also used this same technology to crack passwords through brute-force attacks.

LINK TO LEARNING

In early 2024, the Federal Communications Commission (FCC) made it illegal for companies to use AI-generated voices in robocalls. Read their press release related to voice cloning technology (https://openstax.org/r/109VoiceTech) to learn more about how companies use the technology and why the FCC has made it illegal.

Software updates not only provide new features and improve system performance, they also often deliver critical patches that resolve these vulnerabilities. Cybersecurity demands continuous monitoring and control from a proactive and reactive perspective. Unpatched systems may function normally, which can lead to a false sense of security. Breaches of such systems can compromise the entire network's integrity. The risks include unauthorized data access, identity theft, or even denial of service attacks that can bring business operations to a halt. By understanding the risks posed by software vulnerabilities, organizations can make educated decisions about how to protect their network assets effectively.

Hardware Vulnerabilities

Hardware vulnerabilities can be just as dangerous as software vulnerabilities, but they are often overlooked. A hardware vulnerability is a weakness or flaw within the physical components of a network, such as routers or IoT devices. For example, unsecured routers and other networking devices can be weak points in an organization's cybersecurity defenses. Imagine a router that's still using the default password or is not properly configured; it becomes an easy target for cyberattacks. While it may seem trivial, the hardware that connects your network to the outside world should be as secure as the information it is supporting.

Issues can also arise with IoT devices. These gadgets, such as smart thermostats and smart coffee makers, are increasingly popular but are not always designed with security in mind. Even in an environment where computer systems are well protected, these seemingly harmless devices can be weak points for cyber threats. Without robust security measures, such as strong passwords and regular firmware updates, IoT devices can be manipulated to spy on an organization or serve as a launch pad for broader network attacks. Recognizing these hardware vulnerabilities is the first step toward developing a more comprehensive approach to network security.

Configuration Issues

Poor configuration can be a significant threat to security. Default settings on hardware and software are especially dangerous because they often turn into easy entry points for cybercriminals. For instance, leaving administrative credentials at their factory settings can provide an all-access pass into sensitive systems, compromising the entire network's integrity. Similarly, poorly configured firewalls can be likened to having a state-of-the-art lock but leaving the key under the mat. Even advanced intrusion detection systems become largely ineffective if the firewall rules are not appropriately configured to filter malicious or unnecessary traffic. Poor configurations can lead to unauthorized access, data leaks, and theft of sensitive information.

Real-world incidents have underscored these risks. In 2017, the WannaCry ransomware attack exploited a vulnerability that could have been mitigated with proper security configurations.[5] The malicious software that encrypts users' files such as photos, documents, or other sensitive information and demands a ransom for their release is called **ransomware**. The WannaCry ransomware attack exploited a vulnerability in Microsoft Windows known as "EternalBlue," which allowed the attack to spread across networks, encrypting files along the way (Figure 5.4). Microsoft published a fix for the vulnerability; however, many organizations were slow to make the update, which ultimately resulted in organizations losing billions of dollars. Additionally, numerous data breaches have occurred due to misconfigured cloud storage solutions, exposing sensitive customer data to the public.[6] These incidents serve as cautionary tales, highlighting the need for mindfulness in system and network configurations.

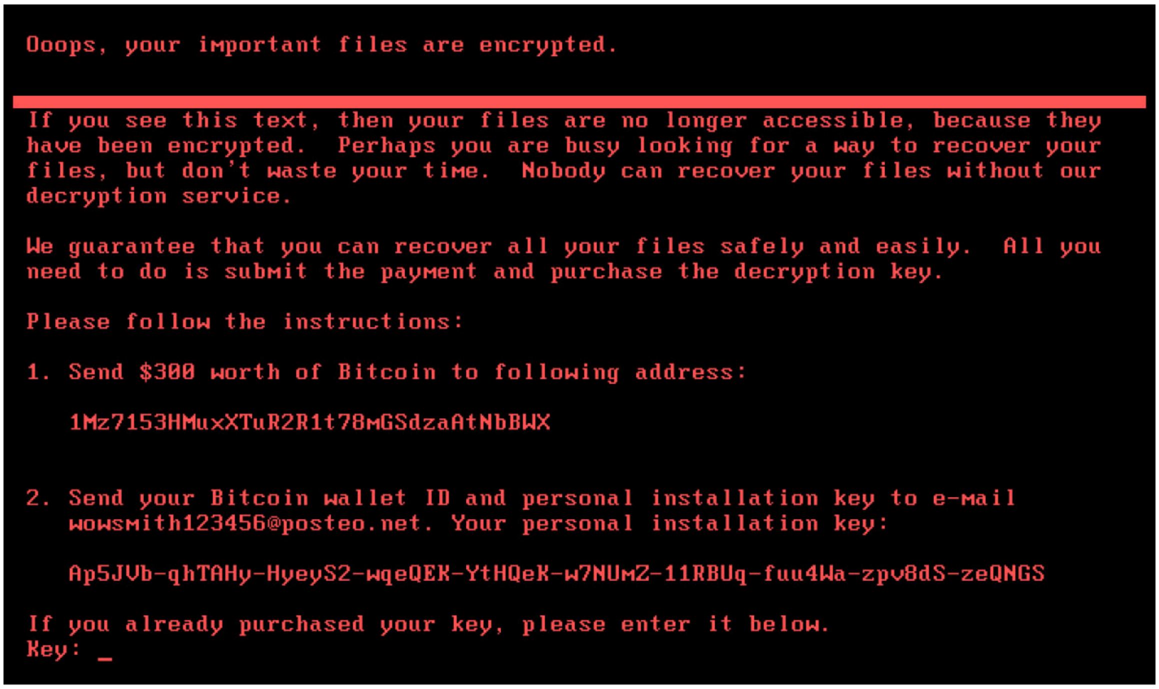


Figure 5.4 Ransomware such as Eternal Blue is malware that encrypts a user's files and demands payment in return for the decryption key. (credit: "Petya (malware)" by Petya/Wikimedia Commons, Public Domain)

Ensuring proper configuration is not just a task for the IT department but requires an organization-wide commitment to adhering to the best practices in cybersecurity. Properly configured settings are the first line of defense in a multilayered security approach, and lapses in this area can have catastrophic implications for any organization.

Types of Network Threats

As we navigate our day-to-day online activities at work, school, or home, there are multiple threats that we must mitigate for our safety. Threats from natural disasters and storms can disable a network, and threats from an external attacker can result in loss of operations or theft. Moreover, an internal threat that originates from within an organization can result in sabotage, data loss, or network compromise. There are three types of network threats: environmental, external, and internal, as Figure 5.5 illustrates.

5 Josh Fruhlinger, "WannaCry Explained: A Perfect Ransomware Storm," CSO, August 24, 2022, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html
6 Edward Kost, "Top 5 Security Misconfigurations Causing Data Breaches," UpGuard, updated November 18, 2024, https://www.upguard.com/blog/security-misconfigurations-causing-data-breaches

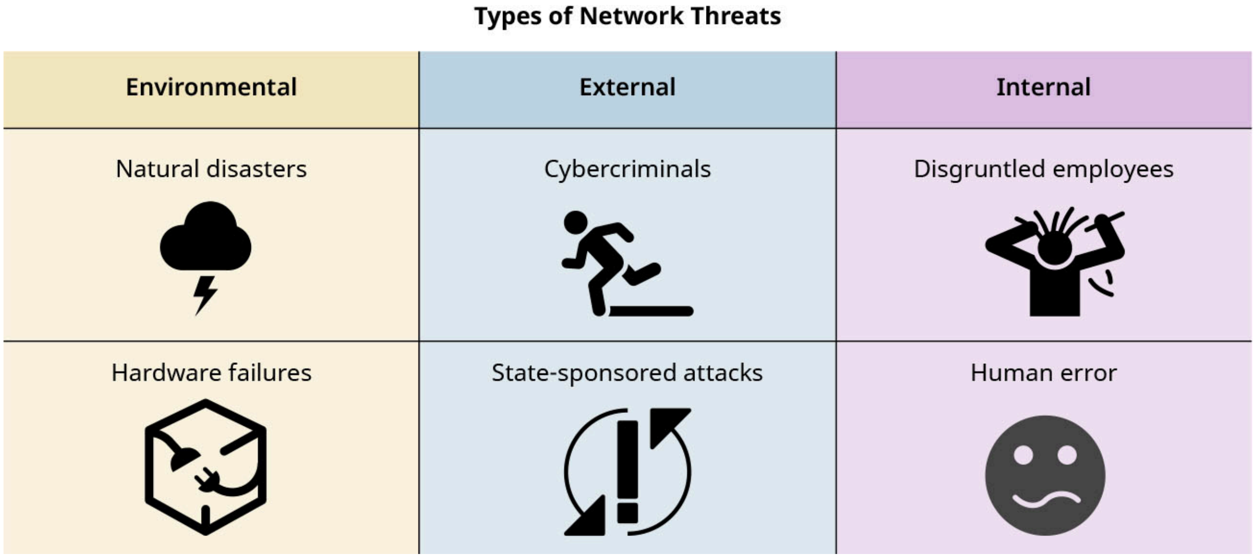


Figure 5.5 Network threats typically fall into three categories: environmental, external, and internal. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit top left: modification of work “Noun storm 2616921” by Uswatun Hasanah/ Wikimedia Commons, CC BY 4.0; credit top middle: modification of work “Noun Project 469419 Run Icon” by Gregor Cresnar/ Wikimedia Commons, CC BY 3.0; credit top right: modification of work “Noun frustration Luis 163554” by Luis Prado/Wikimedia Commons, CC BY 4.0; credit bottom left: modification of work “API - The Noun Project” by “Five by Five”/Wikimedia Commons, CC0 1.0; credit bottom middle: modification of work “Noun Project problems icon 2417098” by “Template, TH”/Wikimedia Commons, CC BY 3.0; credit bottom right: modification of work “Noun confused 274449” by Ben Davis/Wikimedia Commons, CC BY 4.0)

Environmental and External Threats

An **environmental threat** in cybersecurity is an uncontrollable external factor such as a natural disaster or hardware failure that can damage data centers and disrupt business operations. These threats often get overshadowed by the dramatic nature of hacker attacks and internal espionage, yet their impact can be equally catastrophic. For instance, natural disasters such as earthquakes, floods, or hurricanes can severely damage data centers that host critical information and applications. The inability to access or recover this data not only interrupts business operations, but can also have legal and reputational ramifications. Moreover, as these calamities are beyond human control, they are particularly difficult to mitigate. In recent years, the increasing frequency of extreme weather events attributed to climate change has escalated this environmental risk, necessitating an urgent review and adaptation of existing disaster recovery and business continuity plans.[7]

Another common environmental threat is hardware failure. Servers, storage systems, and networking equipment can wear out over time. Without proper monitoring and maintenance, these failures can cause data loss or service interruptions. Unlike natural disasters, hardware failures are often preventable through regular inspections, timely upgrades, and redundancy systems. Many organizations employ real-time monitoring tools that alert them to potential hardware issues before they escalate into full-blown failures. Nonetheless, the commonplace nature of these threats should not lead to complacency; both natural disasters and hardware failures require strategic planning, investment in robust infrastructure, and ongoing vigilance to ensure organizational resilience.

7 Renaud Guidee, “The Next Decade Will Be Defined by Climate Change and Cyber Risk,” World Economic Forum, October 7, 2021, https://www.weforum.org/agenda/2021/10/the-next-decade-will-be-defined-by-climate-change-and-cyber-risks/

An **external threat** in this context refers to a threat that originates from outside an organization, typically posed by cybercriminals or state-sponsored attackers who aim to exploit vulnerabilities for financial or strategic gain. Cybercriminals often appear as resourceful yet malicious actors who continually refine their tactics to evade detection and maximize their gains. Various methods, such as phishing schemes, malware deployment, and ransomware attacks, are among their preferred tools. These individuals or groups are not the only external threats, however; state-sponsored attacks present an even more daunting challenge. Orchestrated by nations aiming to steal critical information or disrupt infrastructures, these attacks benefit from considerable resources and advanced capabilities, turning cybersecurity into a complex game of geopolitics.[8]

Understanding the techniques of these external threats is necessary for developing effective defensive measures. For example, a common method used by cybercriminals is **social engineering**, which involves manipulating employees into revealing sensitive information, often leading to unauthorized system access. At the other end of the spectrum, state-sponsored attacks might employ highly sophisticated methods such as advanced persistent threats (APTs) to gain and maintain long-term access to target networks. These types of threats can include software such as a rootkit or malware. A **rootkit** enables attackers to have access to a system by masquerading as operating system processes, and **malware** is malicious software designed to damage, exploit, or infect systems, or otherwise compromise data, devices, users, or networks, using viruses, worms, and spyware that is installed into the basic input-output system (BIOS) of a computer. While cybercriminals are motivated primarily by financial gains, state-sponsored actors often have a more complex agenda, which could include espionage, destabilization, or strategic advantage. This complexity demands a full understanding, not just of the technological aspects of these threats, but also of the political dimensions that underlie them.

Internal Threats

An **internal threat** is one that originates from within an organization, such as disgruntled employees or poor security training for employees resulting in social engineering attacks. In cybersecurity, internal threats are particularly tricky because they relate to the risk of someone inside a company using their access to systems to cause damage or steal data. While organizations spend a lot on protecting their assets from external hackers, the risks from within can be just as damaging. Disgruntled employees, for instance, already have access to the organization's network and thus can bypass one of the organization's first lines of defense. As the motivations of such people can range from revenge to financial gain, they function as unpredictable actors within the cybersecurity landscape. To further complicate matters, insider threats may not even be intentionally malicious; they could simply be employees who unknowingly compromise security through poor practices, such as using weak passwords or falling victim to phishing scams.

Understanding the risks from internal threats means thinking beyond just technical fixes. The human factor is an important factor. Organizations must create a workplace where employees feel comfortable talking about their concerns. This can help reduce the chances of anyone becoming disgruntled. Simultaneously, companies must implement robust monitoring systems to identify unusual activity that could signal an internal threat. By recognizing the multifaceted nature of internal threats, organizations can develop a holistic strategy that integrates technological, psychological, and administrative measures to safeguard their assets.

FUTURE TECHNOLOGY

The Future of Cyberattacks

Emerging technologies such as quantum computing and AI pose novel threats that organizations must

8 Adam Hunt, "State-Sponsored Cyberattacks Aren't Going Away—Here's How to Defend Your Organization," *Forbes*, May 10, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/05/10/state-sponsored-cyberattacks-arent-going-away---heres-how-to-defend-your-organization/?sh=7acb1aad230b

prepare for. Quantum computing, a method of computing that uses qubits (a measurement of four states as opposed to two), with its unparalleled computational speed, has the potential to break existing encryption algorithms, rendering most current data protection measures obsolete. Initiatives such as post-quantum cryptography are in the works to counter this impending threat, but widespread adoption and implementation remain a challenge.

Alternatively, AI-driven cyberattacks are becoming increasingly sophisticated. Advanced machine learning algorithms can quickly analyze network vulnerabilities and execute complex attacks with little to no human intervention. Moreover, these algorithms can adapt and learn from each cyberattack, making them more effective with each iteration. This intensifies the need for cybersecurity measures to evolve in tandem, incorporating AI-driven threat detection and response systems that can match the capabilities of next-generation threats. Therefore, staying abreast of these future trends is not just advisable; it is imperative for long-term security resilience.

5.2 Security Technologies and Solutions

Learning Objectives

By the end of this section, you will be able to:

- Identify technologies and solutions to protect information and networks
- Identify potential security threats and vulnerabilities, and choose appropriate countermeasures
- Describe best practices for secure computing and risk management
- Determine legal and ethical issues in securing information and networks

As technology continues to advance, protecting digital information and networks has become a top priority for individuals, organizations, and governments alike. With the rise of increasingly sophisticated cyber threats, it is essential to understand the tools and strategies available to safeguard sensitive data and critical infrastructure. Effective security requires not only the right technologies to defend against potential attacks, but also a solid understanding of how to identify vulnerabilities and implement measures that mitigate risk. In addition to technical solutions, secure computing practices and thoughtful risk management play a crucial role in maintaining system integrity. Furthermore, navigating the complex landscape of legal and ethical issues surrounding information security is vital, as the balance between privacy, compliance, and protection continues to evolve.

Technologies and Solutions to Protect Information and Networks

In cybersecurity, numerous technologies and solutions stand as defenses against an array of threats that aim to compromise information and network security. The field of **information security risk management (ISRM)** involves identifying, assessing, and mitigating risks to the confidentiality, integrity, and availability of information and information systems. From foundational measures such as firewalls and encryption protocols to specialized tools for intrusion detection and risk assessment, the complexities of maintaining a secure digital environment are wide-ranging. These technologies play critical roles in safeguarding both individual and organizational digital assets. Furthermore, these technologies can enable ISRM professionals to promote digital trust, a valuable tool for growth and success of businesses.

Firewalls

Firewalls serve an important role in network security, functioning as the gatekeepers that police the flow of data coming in and out of a network. Acting as the first line of defense, they are necessary in preventing potential cyber threats from external sources. The versatility of modern firewalls allows for a comprehensive approach to managing data flow. Advanced versions meticulously examine the content within a **data packet**, which is a small unit of data transmitted over a network, and differentiate various forms of web traffic such as file transfers, browser activity, and applications accessing the internet, thus facilitating the implementation of nuanced security policies.

For instance, firewalls can authorize access to applications that have undergone rigorous vetting processes and are deemed safe while promptly blocking others that pose a potential security risk. These applications vary, ranging from video games seeking updates to activity in the background while browsing the internet.

Types of Firewalls

There are several types of firewalls, each with a distinct set of features and functionalities, but they are broadly categorized into hardware and software firewalls. The most basic type of firewall is a packet filtering firewall, which checks the header of packets as they pass through, looking for specific characteristics such as source and destination address, port number, and protocol used. They are usually software based, and they operate by examining packets of data to determine whether to allow them through based on preset rules.

A more advanced type of firewall is a stateful inspection firewall, which monitors active connections and uses that context to block or allow connections. These types of firewalls may be software or hardware based. A next-generation firewall (NGFW) is an advanced type of firewall that provides more comprehensive security features than traditional packet filtering and stateful inspection and uses a proactive approach to network security. These firewalls come equipped with integrated intrusion detection and prevention systems (IDPSs), offering an additional layer of security. These IDPS functionalities are engineered to actively scan for, identify, and neutralize known threats as they occur.

A proxy firewall is a network security device that filters incoming and outgoing traffic by acting as an intermediary between users and the web. It is software based and provides an additional layer of isolation and security.

Firewall Implementation Challenges

Firewalls are essential for **network security**, which is the process of guarding network infrastructure and IT systems from unauthorized access, misuse, malfunction, or improper disclosure to unintended parties. It involves using a variety of tools, technologies, and policies to ensure the safety and security of data traveling over the network. Configuring detailed security policies can get complicated, and there is a risk of false positives in intrusion detection. Plus, firewalls need regular updates to handle new threats, so they require ongoing maintenance. Despite these challenges, firewalls are an important part of any solid network security plan. To boost cybersecurity, it is smart to have backup plans in place. This also goes for hardware. Using two different firewalls from two different providers can add extra layers of protection and reliability.

Protocols

A **protocol** is a fundamental rule or procedure that governs communication between devices in a network. Protocols ensure that data are transmitted accurately, reliably, and securely by defining how data are packaged, transmitted, and received. Protocols operate at various layers of the network stack, addressing different aspects of communication. By standardizing communication processes, protocols enable interoperability between different systems and devices, making seamless and efficient digital communication possible. Think of them as rules that computers must obey, like how drivers must obey traffic laws. Common protocols include HTTP, HTTPS, VPN, and S/MIME.

Hypertext Transfer Protocol (HTTP) and its secure alternative HTTP secure (HTTPS) form the foundation of web communications (Table 5.2). **Hypertext Transfer Protocol (HTTP)** is proficient at transmitting hypertext over the internet, and **Hypertext Transfer Protocol Secure (HTTPS)** adds a secure, encrypted layer to HTTP via SSL/TLS protocols. To understand how HTTP works, imagine that you make a request for a web page through a browser. This happens when you click on a link or enter an address in the search bar of your browser, initiating an HTTP request. This request is sent to a web server, which then responds by supplying the requested information in the form of hypertext. This hypertext is what your browser interprets and displays as a web page. The process is remarkably fast, enabling standardized and consistent viewing of websites across different browsers. Encrypting a connection ensures that the data in transit is secure. For ISRM professionals, understanding the importance of HTTPS over HTTP is essential, especially when dealing with sensitive information.

	HTTP	HTTPS
Security	Data are sent in plain text, making them vulnerable to interception	Data are encrypted, ensuring privacy and security; uses SSL/TLS protocols
Port	80	443
URL prefix	URLs begin with http://	URLs begin with https://
Trust	Does not provide a certificate to verify the website’s identity	Provides a digital certificate issued by a certificate authority (CA)

Table 5.2 Comparing HTTP and HTTPS HTTPS provides much more security, whereas HTTP provides little to no protection.

Virtual private networks (VPNs) serve as a proxy for internet communication by establishing a private encrypted connection or tunnel that makes it difficult for attackers to breach. Various protocols such as Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and OpenVPN are used for different security and speed requirements. PPTP is fast but less secure, whereas OpenVPN offers a balance of speed and security. L2TP usually operates with IPsec for added security.

A Secure/Multipurpose Internet Mail Extension (S/MIME) is a standard for public key encryption and signing of MIME data. It is frequently used for securing email messages. S/MIME allows for cryptographic security services such as authentication and message integrity checks, ensuring that both the sender and the information remain uncompromised.

Intrusion Detection and Prevention Systems

In network security, an **intrusion detection and prevention system (IDPS)** monitors networks for malicious activity or policy violations. This is vital for keeping information secure. Think of protocols as a set of rules that allow machines to communicate smoothly. IDPSs, on the other hand, are specialized hardware and software tools that monitor network traffic to detect and prevent security breaches. These systems come in various forms and can be deployed in different ways to best protect against potential threats. By actively monitoring communications, IDPSs help prevent security incidents before they can cause harm. Signature-based IDPSs are designed to detect known threats by searching for specific patterns, such as malware signatures. Anomaly-based systems, on the other hand, focus on identifying abnormal patterns in data flow or behavior that might signify a security threat. Both have their own advantages and limitations; signature-based systems are highly effective against known threats but can miss new, previously unseen threats, while anomaly-based systems can detect novel threats but are prone to false positives.

Network-based IDPSs are used to monitor and analyze network traffic to protect an entire network from threats, whereas host-based systems are installed on individual devices and protect against unauthorized data manipulation or software vulnerabilities specific to those devices. These systems often rely on signature-based detection methods along with anomaly-based methods that look for unusual patterns in network traffic that could be harmful.

Monitoring Tools

The foundation of an effective information security strategy begins with simple and effective monitoring tools, such as log files, alarms, and keyloggers. Although these measures might appear basic, their importance cannot be overstated, especially when it comes to instilling a sense of digital trust.

A **log file** is a file generated by security applications that contains event information that aids in determining the status and health of a network. These are invaluable for diagnostics, troubleshooting, and security audits. An alarm is a protection device often installed on equipment to notify staff in the event of tampering or breach. It serves as a real-time alert system that notifies administrators of potential security threats. These are usually triggered by predefined conditions set within the IDPS or other security software. A **keylogger** is a tool or technology often used maliciously to capture keystrokes on a computer to obtain sensitive information such as passwords. Although they are often associated with malicious activities, legitimate versions exist for monitoring and auditing purposes. However, these tools must be managed carefully to ensure they do not compromise the very security they are meant to uphold.

In addition, the following tools are also used for monitoring network security:

- A **packet sniffer**, also known as a network analyzer or protocol analyzer, is a tool that captures and analyzes network traffic. It intercepts data packets flowing across a network, allowing for examination of the data within these packets, including their source, destination, and content. Packet sniffers can capture data packets in "promiscuous mode," meaning they can see all traffic on the network, not just traffic intended for the sniffing device. For example, Wireshark is a popular open-source packet analyzer that allows capture and analysis of network traffic.
- A **protocol analyzer** is a tool that examines network communication protocols to understand how data are exchanged between devices and applications on a network. Protocol analyzers capture and analyze data packets, decode them based on the protocol used, and provide insights into the communication process. They can identify errors, performance bottlenecks, and security vulnerabilities related to specific protocols. Protocol analyzers and packet sniffers are often used interchangeably, as they both involve capturing and analyzing network traffic. However, protocol analyzers focus more on understanding the communication protocols and analyzing the data within the context of those protocols.
- A **security information and event management (SIEM)** system is a security solution that collects, analyzes, and correlates security data from different sources to detect and respond to security threats in real time. SIEM systems gather logs, events, and alerts from various security tools and network devices, and then use advanced analytics to identify suspicious activity, potential vulnerabilities, and security incidents. SIEM helps organizations improve threat detection, incident response, security compliance, and overall security posture.

Best Practices for Network Threat Mitigation

In the complex domain of information security, best practices serve as guiding principles that are universally applicable across various sectors and organizational structures. They are the reliable methods that provide consistent security outcomes and contribute to the establishment of digital trust. Best practices in the information security field include the following:

- multi factor authentication (MFA), which adds an additional layer, or layers, of security, ensuring that even if one factor is compromised, unauthorized access is still restricted
- regular updates and patch management, the routine process of updating software to address security vulnerabilities, are ongoing, proactive measures that attempt to close the gap through which cyberattackers can infiltrate systems
- zero trust, or "never trust, always verify," a cybersecurity model where access to resources is granted based on strict verification and continuous authentication, rather than assuming trust based on network location or device ownership

- defense in depth, a cybersecurity strategy that employs multiple layers of security controls to protect against attacks, so that if one layer fails, others will still be in place to prevent a breach
- vendor diversity, the practice of using multiple vendors for different security products and services instead of relying on a single vendor to mitigate risks associated with vendor lock-in, reduce security vulnerabilities, and improve overall security posture
- security training and awareness programs, which educate employees about the importance of information security, the role they play in safeguarding organizational assets, and how to recognize phishing attempts, maintain password integrity, and ensure secure data transmission

The human element is often regarded as the weakest link in the security chain. By adopting these best practices, information security and risk management professionals not only enhance an organization's resilience against internal and external cyber threats, they also contribute positively to building digital trust, thereby enabling business to grow and thrive in an increasingly interconnected world.

Security Threats, Vulnerabilities, and Appropriate Countermeasures

Security threats and vulnerabilities are constantly changing, posing an ongoing challenge for organizations and individuals alike. As the IoT, machine learning algorithms, and other technologies integrate deeper into our lives, they offer an attack surface for malicious actors. The stakes are not just financial or operational; they traverse digital trust, which is a confidence in the ability of processes, technology, and organizations to create a secure digital world. Digital trust is a valuable notion that protects organizational branding and confidence. When digital trust is compromised, it significantly impacts the organization and its stakeholders, including customers, partners, and regulators.

For example, in 2024, New Hampshire voters filed a lawsuit against the creators of a deepfake robocall that used AI to generate a fake audio message of former president Joe Biden asking voters to stay home and not go to the voting booths or poll stations.[9] Conceptually, such deepfake scams typically involve creating realistic audio or video imitations of trusted figures to deceive individuals into taking unauthorized actions. When these scams are uncovered, consumers lose their digital trust in the organization that created them. People are naturally protective of their assets, valuables, and identity, all of which they perceive as threatened when they see an organization misusing digital assets. Through a detailed understanding and implementation of security mechanisms, individuals and organizations can defend against threats and build resilient systems that adapt to new challenges as they arise.

Types of Threats

As the internet has gathered more users over the last few decades, cyberattacks have significantly increased. These attacks vary greatly, consisting of password attacks, phishing attempts, Trojan viruses, malware, and ransomware that holds users' sensitive files hostage for ransom payment. Understanding these attacks and how to prevent them is key to information security.

As the most fundamental of access controls, passwords are a frequent target of malicious actors. Two primary types of password attacks exploit weaknesses in password security: brute-force attacks and dictionary attacks. In a **brute-force attack**, an attacker systematically checks all password or encryption key possibilities until the correct one is found. In contrast, a **dictionary attack** uses a precompiled list of likely passwords. Imagine trying to crack a padlock with four digits, each ranging from 0 to 9. If you don't have any hints, you'd have to try every possible combination, which adds up to 10,000 different permutations (10^4), which is a lot of guessing.

Now, consider a dictionary attack. Instead of trying every single combination, a dictionary attack gives you a list of likely combinations based on common patterns or known sequences. This way, you might find the

9 Ali Swenson and Will Weissert, "New Hampshire Investigating Fake Biden Robocall Meant to Discourage Voters Ahead of Primary," *Associated Press*, updated January 22, 2024, https://apnews.com/article/new-hampshire-primary-biden-ai-deepfake-robocall-f3469ceb6dd613079092287994663db5

correct code faster. To guard against both types of attacks, organizations implement stringent password policies that encourage complex combinations, and they use MFA.

Phishing attacks aim to trick individuals into revealing sensitive information. The attacker often masquerades as a trustworthy entity, employing emails or messages (Figure 5.6) that prompt users to enter passwords or other confidential data. Implementing robust email filtering technology and educating users about the elements of phishing schemes are critical components of a well-rounded defense strategy.

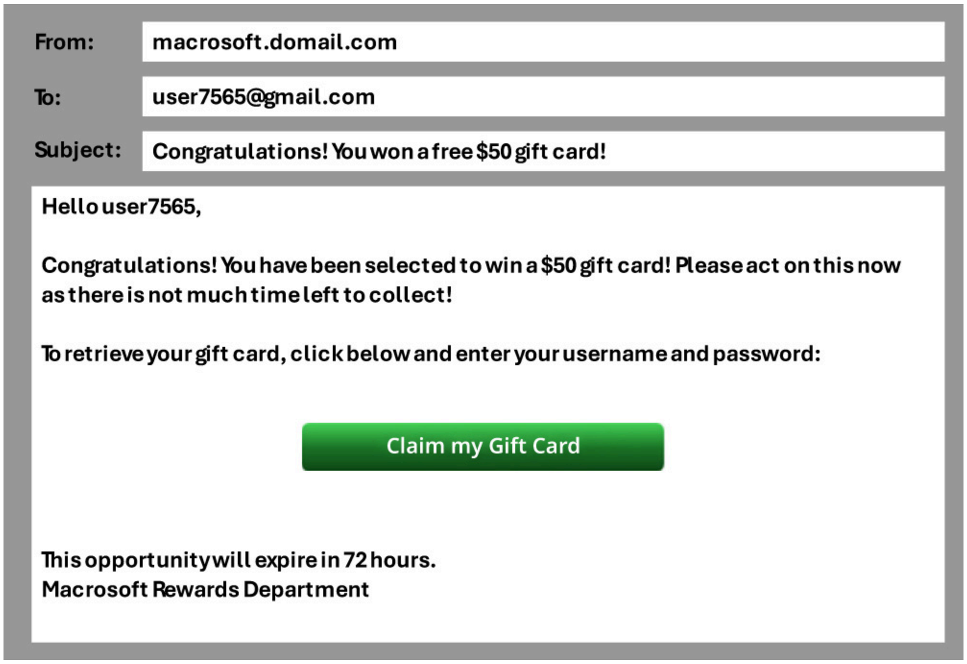


Figure 5.6 Many phishing attempts will appear to originate from a trusted source. However, on careful inspection, one can notice several discrepancies that discredit the attempt. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

By weaving these basic security measures into an integrated strategy, ISRM professionals can better arm organizations against a range of threats. Simple security measures serve both as a first line of defense and as foundational elements that support more complex security protocols. This layered approach to security helps maintain digital trust, fostering an environment where businesses can operate with greater confidence in the digital realm.

Among the most frequently encountered security threats are malware variants such as viruses, worms, and Trojans (Figure 5.7). A **virus** attaches itself to clean files and propagates to other files and programs. A **worm** is a stand-alone software program that spreads without requiring a host program. A **Trojan** is a program that conceals itself as a safe program but often carries many other different types of malicious payloads.

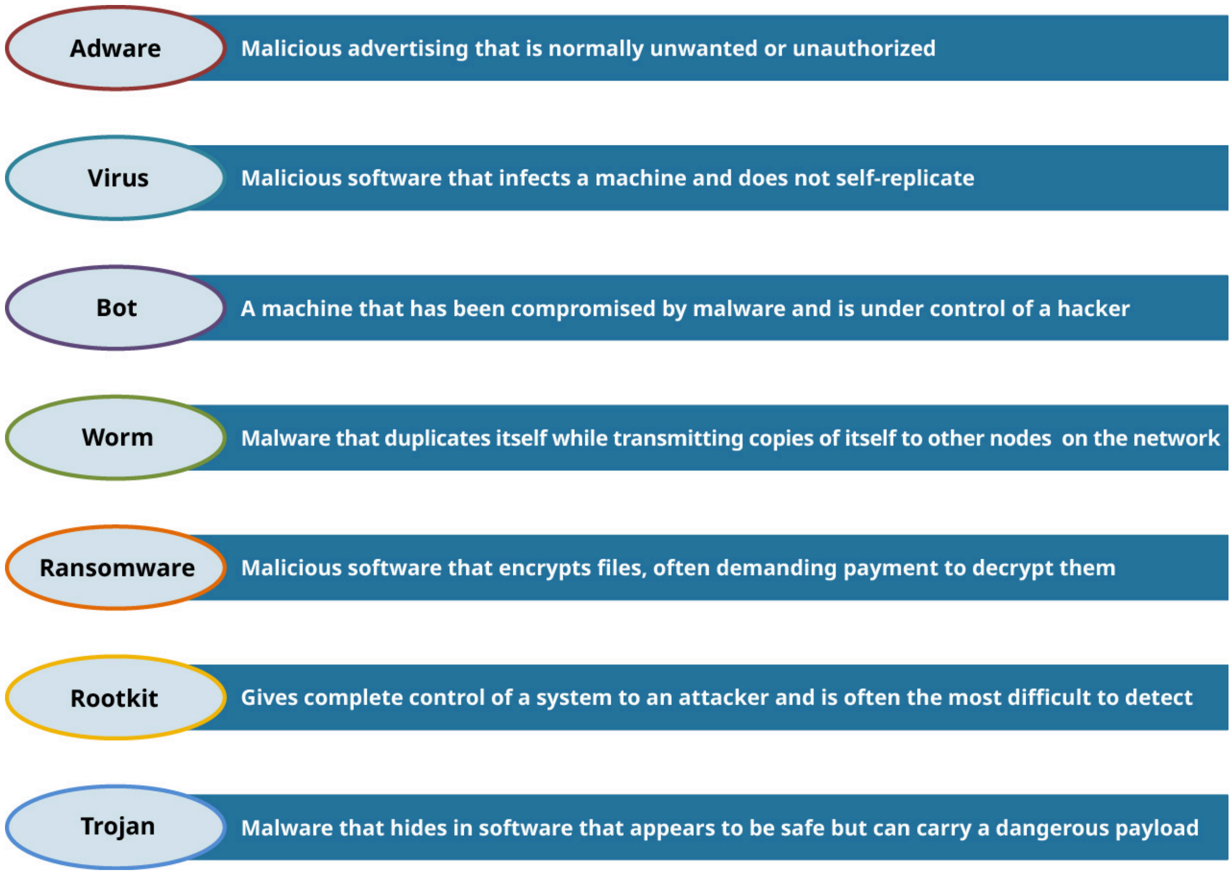


Figure 5.7 While not an exhaustive list of malware, these are the most common types. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Malware such as Trojan horses and ransomware represent more sophisticated external threats. Trojans trick users into willingly downloading malicious software that is often disguised as a legitimate program. The software provides attackers unauthorized access to systems. Advanced endpoint security solutions coupled with regular updates and patches can offer significant protection against these types of malware.

In recent years, more insidious forms of malware such as fileless malware have emerged. Unlike traditional malware, which relies on files stored on the hard disk, **fileless malware** exploits in-memory processes to conduct its nefarious activities. By leveraging legitimate system tools such as PowerShell or Windows Management Instrumentation, fileless malware conducts operations entirely within the device's random access memory (RAM), leaving little to no footprint on the hard disk. This makes it significantly more challenging for traditional antivirus solutions to detect and eliminate. For a better understanding of how fileless malware works, look at how Figure 5.8 follows a user's click in a spam email.

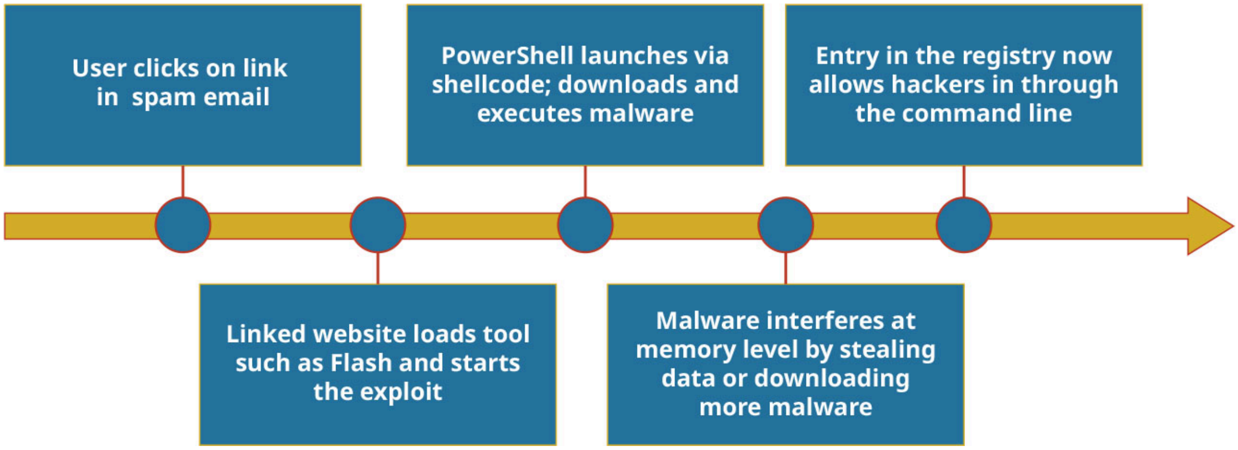


Figure 5.8 This example demonstrates how fileless malware operates. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

In contrast to software-based threats, which target vulnerabilities in computer systems, social engineering attacks such as phishing and pretexting leverage human vulnerabilities. A social engineering attack includes deceptive tactics used to manipulate individuals into divulging confidential information, exemplified by phishing and pretexting. Phishing usually involves sending deceptive emails to trick employees into revealing sensitive information. On the other hand, **pretexting** involves creating a fabricated scenario to obtain private data. Despite the sophistication of technical countermeasures, the human factor remains a vulnerability, making these types of attacks especially harmful to the establishment of digital trust.

An insider threat is a risk posed by individuals within an organization who have access to sensitive information and systems; they warrant special attention because employees or contractors with insider information can perpetrate or facilitate attacks that may bypass conventional security measures. This “inside advantage” makes the threat more complex, as mitigating such threats requires a blend of technical controls and organizational policies.[10] Some of these policies include actions such as mandatory vacations to prevent fraud, role-based access controls that limit employee access to sensitive information, security awareness training, and regular audits.

A **distributed denial-of-service (DDoS)** is an attack that uses multiple computers or servers to overwhelm a network, resulting in loss of usability. These pose a unique threat: unlike other attacks that seek to gain unauthorized access or retrieve sensitive information, DDoS attacks aim to incapacitate the target’s operations. The immediate impact is not just operational disruption, but also a severe degradation of digital trust among stakeholders.

Vulnerabilities

One of the most well-known software vulnerabilities is the **buffer overflow**, a condition where an application writes more data to a buffer than it can hold. This results in data corruption and could allow an attacker to execute arbitrary code. Another common vulnerability is Structured Query Language (SQL) injection, which occurs when attackers insert or manipulate SQL queries in an input field, allowing them to gain unauthorized access to a database. This kind of attack can lead to data leaks, loss of data integrity, and other security issues.

Attacks on firmware (hardware) are increasingly prevalent. These are more difficult to detect as they target the device at the BIOS or firmware level. This also makes it harder to remove the malware once in the system. Physical tampering, while straightforward, is another hardware vulnerability. Unauthorized physical access to hardware can result in the installation of keyloggers or data extraction.

10 Cybersecurity and Infrastructure Security Agency, “Defining Insider Threats,” accessed October 12, 2023, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Although cyber threats often originate from the application of sophisticated hacking techniques, it is not uncommon that the root cause of a breach can be traced back to a simple configuration error. The T-Mobile data breach of 2023, where a third of its customer base had private information exposed, shows what can occur when application programming interface (API) configurations are not sufficiently secured.[11] An API is a set of protocols, tools, and definitions that enable different software applications to communicate and interact with each other, allowing for the exchange of data and functionality. In this breach, insecure APIs allowed threat actors to access sensitive customer data, impacting not just the affected individuals, but also T-Mobile's reputation. As more companies transition their services to the cloud, the risk posed by insecure API configurations is escalating.

Countermeasures for Threats

Countermeasures to mitigate cybersecurity threats involve a diverse set of tools and approaches. They often need to be tailored to the specific types of threats and vulnerabilities that an organization faces, but some universally applicable solutions have proven effective across multiple sectors.

- Antivirus and anti-malware software: The most basic but critical line of defense is antivirus and anti-malware software. These programs provide real-time protection against known threats and offer heuristic analysis to detect previously unknown forms of malware.
- Employee training and awareness: Human error remains one of the most significant vulnerabilities in any organization. Phishing simulations and awareness training can drastically reduce the likelihood of an employee inadvertently compromising security. A 2024 study has shown that a combination of phishing awareness programs and phishing testing programs can significantly reduce the click-through rate on phishing emails.[12]
- Intrusion detection systems: An intrusion detection and prevention system is vital to monitoring network behavior for unusual or suspicious activity.
- Access control policies: One method of access control, **role-based access control (RBAC)**, bases data access on a person's role in the organization, giving each employee the minimum level of access they need to perform their job functions. This requires an organization to maintain a complete list of data elements combined with a list of viewable roles and attributes. For example, a health-care organization can successfully thwart an internal threat by limiting access to patient records to only those employees who require it for their job duties. Given the complexity and ever-evolving nature of cyber threats, these countermeasures serve as foundational elements in the continuous effort to uphold digital trust.
- Regular software patching: One of the most effective ways to mitigate vulnerabilities is through timely software patching. In 2017, the WannaCry ransomware attack exploited a vulnerability in older Windows systems. Microsoft had issued a patch months before, but because many organizations had not updated their systems, this led to widespread damage.[13]
- Physical security measures: Physical intrusion can bypass the most sophisticated digital security measures. One type of social engineering known as tailgating is a good example of this. Tailgating is the act of following someone very closely as they enter a secured building. This enables the attacker to enter the facility without having to use credentials such as an ID badge. Once inside, the attacker has access to critical infrastructure and can cause a data breach or other damage. Strict controls such as mantraps, which prevent more than one person from entering a facility simultaneously, help to mitigate this threat.

Additional Practices for Secure Computing and Risk Management

Cybersecurity threats are always changing, and vulnerabilities can pop up when least expected. That is why

11 "T-Mobile Informing Impacted Customers about Unauthorized Activity," T-Mobile, January 19, 2023, https://www.t-mobile.com/news/business/customer-information
12 Gry Myrtveit Gundersen, "Does Phishing Training Work? Yes! Here's Proof," *CyberPilot*, January 5, 2024, https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof
13 Josh Fruhlinger, "WannaCry Explained: A Perfect Ransomware Storm," CSO, August 24, 2022, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html

prevention should be the cornerstone of any threat mitigation strategy. Organizations need to tackle cyber threats with proactive strategies, using secure computing and risk management practices that are both thorough and flexible.

Ethical Hacking

The process of attempting to break into an organization's computer systems, network, or applications with permission to identify vulnerabilities is called **ethical hacking**. It has gained considerable attention as a much-needed practice within the cybersecurity field. While the goals of ethical hackers align with those of cybersecurity experts in identifying vulnerabilities, the methods employed can resemble those of malicious hackers. This raises questions regarding the ethical and legal boundaries that distinguish ethical hacking from unauthorized, illegal activities.

The concept of consent is fundamental in ethical hacking. Unlike malicious actors, ethical hackers operate with explicit permission from the organization that owns the system. This consent is often given under a legal contract that outlines the extent of the testing, the systems that can be assessed, and the methods that can be used. Consent provides the ethical and legal basis for the hacking activities, turning what could otherwise be considered an illegal breach into an accepted practice.

One example that illustrates the gray area in ethical hacking is a 2019 case involving a cybersecurity firm. Two of its ethical hackers were arrested in Iowa while conducting a physical security assessment of a courthouse. Despite their having a contract that permitted them to perform physical intrusion testing, the authorities arrested them, and the hackers faced criminal charges. This was particularly surprising because the cybersecurity company had been hired by Iowa's judicial branch to conduct the assessment.[14]

This incident highlighted the potential ambiguity and legal risks involved in ethical hacking, even when it's conducted under a contract. It sparked an extensive debate in the cybersecurity community about the legal safeguards needed for ethical hackers. The charges against the two ethical hackers were eventually dropped, but not without the individuals and the firm suffering reputational damage. The case became a watershed moment for ethical hacking, urging the community, lawmakers, and organizations to be more explicit in contracts and to establish clearer legal guidelines.

This case serves as reminder that ethical hacking is a field still very much in the process of defining its legal and ethical contours. There is a clear need for explicit and transparent guidelines for ethical hackers and legislators, and they need to maintain an ongoing dialogue to build a more robust legal framework.

CAREERS IN IS

The Role of Ethical Hackers

Ethical hackers are security professionals with specialized training in simulating cyberattacks under controlled conditions. Their role is to systematically assess the security posture of an organization by conducting targeted tests first to identify and then to exploit vulnerabilities in software, hardware, and operational procedures. They conduct penetration testing that simulates real attacks by scanning systems, then attempting to breach them, and then determining how deep they can get into the system. Ethical hackers can also perform security audits and assessments and report the results of their penetration testing and audits to the organization with recommendations for improving the security. An organization may also hire an ethical hacker for continuous monitoring. Their work must fall within all laws and standards, following guidelines from the Open Web Application Security Project (OWASP) or standards from the National Institute of Standards and Technology (NIST). All ethical hackers must have authorization from the organization, maintain integrity of the system and data, and maintain confidentiality when handling

14 Faegre Baker Daniels, "Coalfire Investigation Report," October 9, 2019, https://www.iowacourts.gov/collections/445/files/919/embedDocument

data.

Risk Management Approaches

Risk assessments are important for identifying vulnerabilities and determining how they impact organizational objectives. These assessments can be either quantitative or qualitative in nature (Table 5.3).

Qualitative Risk Assessment	Quantitative Risk Assessment
Uses subjective criteria such as expert opinions and likelihood scales	Uses numerical data and statistical methods
Uses data from interviews and observations	Uses measurable data such as historical records and figures
Usually returns more descriptive insights	Information returned is generally descriptive in nature
Requires less in terms of tools for analysis	Normally requires more resources and analysis tools
Suited best for situations where exact data are not available	Preferred for risks that can be accurately measured

Table 5.3 Comparison of Qualitative and Quantitative Risk Assessments Qualitative assessments are subjective, whereas quantitative assessments are objective.

Before organizations can assess risks, they should try to determine two factors: their appetite for it and their level of tolerance. A **risk appetite** refers to the level of risk an organization is willing to accept in pursuit of its ambitions or goals and is more qualitative in nature. It is a strategic outlook set by top management and influences how resources for security measures are allocated. Unlike risk appetite, **risk tolerance** is the number of unfavorable outcomes an organization is willing to accept while pursuing goals and other objectives. It is more operational and quantitative than risk appetite, using statistical probability to identify potential risk outcomes. It defines the boundaries of risk variations that are acceptable during the execution of specific projects or processes. In a cybersecurity setting, addressing risk tolerance could include prioritization strategies on how resources are allocated on a network, the network credentials of employees, and budget allocation for IT management. One example of this is a company that allows their ethical hackers to monitor malicious and dangerous sites to identify potential threats. While this is a proactive approach to identifying new threats, monitoring outside threats does not come with the same explicit permission an ethical hacker would have to penetrate the organization's systems. The hacker would need to be especially careful not to violate the site's terms of service or acceptable use policies.

Frameworks for Risk Management

In the world of information security, frameworks play a very important role in managing and controlling risks. A framework is a structured set of guidelines and best practices that help an organization to implement, manage, and maintain security protocols. There are many frameworks to guide risk management practices. One recognized model is NIST's Cybersecurity Framework. The NIST framework is widely adopted due to its user-friendly nature and applicability across many sectors. Moreover, it aligns well with other standards and is scalable to the size of the industry. The NIST framework is divided into five core functions (Figure 5.9).

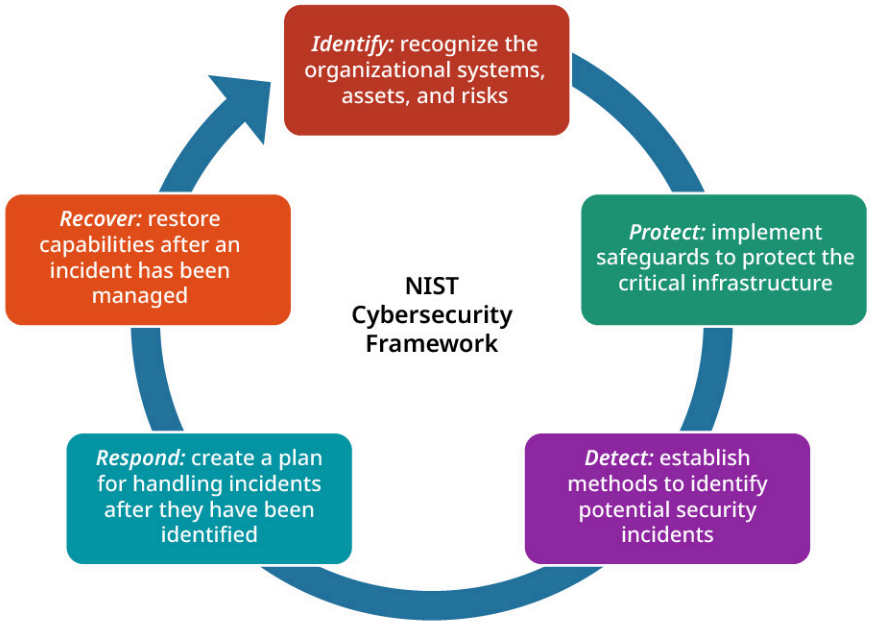


Figure 5.9 The five steps of the NIST process for risk management are to identify, protect, detect, respond, and recover. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The NIST framework provides a flexible and cost-effective approach to improving cybersecurity across industries. It is designed to be adaptable to organizations of all sizes and is widely used to strengthen cyber defenses.

Building a Culture of Security

As you've learned, human error or negligence often poses a significant information security risk. Implementing technical solutions is only part of the equation; the other part lies in fostering a strong security culture within an organization. Training programs and regular awareness sessions can provide employees with the necessary skills and knowledge they need to serve as the organization's first line of defense. Training can help them recognize phishing attempts, use strong passwords, and follow security best practices. Educating staff on proper behavior is key to reducing the risk of human error and preventing security breaches.

Legal and Ethical Issues in Securing Information and Networks

Compliance with laws and regulations is a required aspect of cybersecurity. These regulations not only protect the digital privacy of citizens, but also provide a mechanism of action for those whose rights are violated. Some examples of regulations are the General Data Protection Regulation (GDPR), which impacts data storage and sharing practices within the EU, and the Payment Card Industry Data Security Standard (PCI DSS), which lays out regulations for organizations that handle credit card transactions. As new threats emerge, regulations like these can change frequently, especially as attackers gain access to new technologies and attack methods. Being caught not complying with regulations can lead to heavy penalties or even legal action. Thus, regular updates and audits are vital in ensuring continuous compliance with current regulations.

Understanding the relationship between legal frameworks and ethical considerations is critical for legal compliance and maintaining stakeholder trust and safeguarding organizational reputation. With the expansion of digital technologies into every aspect of daily life, compliance with legal and ethical norms and guidelines becomes not just advisable but essential. Not adhering properly to such norms or guidelines can result in severe ramifications, ranging from legal penalties to a loss of customer trust. Moreover, noncompliance can irreparably harm an organization's standing in the global market.

Legal Protections Afforded to Employees and Users

There are legal guidelines in place that affect every stakeholder in an organization to protect them from harm.

Understanding these protections is essential for organizations to protect their users, human capital, and assets. Increasingly, employees who report cybersecurity lapses are protected by whistleblower laws. This protection introduces an additional layer of legal complexity for organizations. Disciplinary actions against employees who report cybersecurity issues can lead to legal repercussions, such as lawsuits and regulatory action. One way to avoid such situations is to emphasize the need for a robust internal reporting and response mechanism.

User Agreements and Legal Recourse

End-user license agreements (EULAs) and terms of service (ToS) often contain clauses related to data security and privacy. However, these agreements are coming under increasing scrutiny for being “contracts of adhesion,” giving consumers little negotiating power. In the context of cybersecurity, these agreements frequently encompass clauses specifically related to data security and privacy, outlining the responsibilities of service providers in protecting user data and detailing the measures taken to prevent data breaches and cyberattacks.

As cybersecurity incidents become more prevalent, courts are beginning to scrutinize these agreements more closely, particularly assessing whether they provide adequate protection to users against cybersecurity threats. This shift in legal perspective is significant as it could lead to more stringent requirements for cybersecurity measures in user agreements, offering enhanced legal recourse to consumers in cases of lax cybersecurity practices. The evolving legal landscape around EULAs and ToS underscores the need for robust cybersecurity measures and fair user agreements to maintain digital trust and legal compliance.

Regional Laws, Intellectual Property Rights, and Consequences

Regional laws and their implications can serve as critical indicators of how various jurisdictions respond to the challenges posed by cybersecurity and data protection. In the United States, for instance, the California Consumer Privacy Act (CCPA) serves as a legislative example that is often considered to be the most stringent data protection law in the country. Not only does it allow Californians to understand what personal data are being collected about them, it also gives them the ability to deny the sale of their data.[15]

One of the most challenging aspects of cybersecurity law is the notion of jurisdiction in cyberspace. An organization based in one country may store data or have data centers in another. This poses questions about which laws apply and how they can be enforced. For instance, a European company with U.S.-based clients will need to consider both GDPR and any relevant U.S. laws.

Navigating jurisdictional conflicts can be quite complex for organizations. To handle these challenges effectively, it is essential to have a solid grasp of international law as it applies to cyberspace. This knowledge is becoming increasingly important as businesses expand globally, each country bringing its own set of regulations and requirements. Staying current with these diverse legal landscapes is not just good practice, it is necessary for maintaining compliance and ethical standards in today’s digital world. GPDR and laws like it have had a major impact on how companies respond to takedown requests for data and how they protect data in storage and transit. Failure to comply with these regulations has resulted in substantial fines.

LINK TO LEARNING

TechTarget provides news and trending topics (https://openstax.org/r/109TechTarget) in security.

Intellectual property rights, particularly copyright laws, are a crucial element in the digital domain. These laws grant the creators of original works exclusive rights to their intellectual property, allowing them to control the distribution, modification, and public performance of their creations. In cybersecurity, this can include

15 “AB-375 Privacy: Personal Information: Businesses,” California Legislative Information, June 29, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

software code, databases, and even certain types of algorithms, beyond the more traditional forms of media such as text, images, and music.

Copyright infringement in the digital age has developed into an important topic due to the ease of data replication and dissemination. Whether it is pirated software, illegal downloading of copyrighted music or movies, or unauthorized distribution of proprietary information, infringement can have a significant financial impact for an organization that relies heavily on copyrighted material for their business operations. They can lose substantial revenue, which could, in turn, affect their ability to innovate and compete. The legal consequences for infringement can range from fines to imprisonment.

Moreover, copyright infringement can result in a cascade of legal disputes that may involve multiple jurisdictions, especially if the data are stored or transmitted across borders. This complexity can strain resources as companies are forced to engage in lengthy and costly legal battles. For cybersecurity professionals, understanding the subtleties of copyright laws and their enforcement mechanisms is essential not just for risk mitigation, but also for ensuring ethical conduct in an organization's digital operations. This underscores the need for a robust copyright protection strategy as a part of an organization's overall cybersecurity posture.

In addition to copyright infringement, organizations face substantial legal consequences for failing to protect intellectual property (IP). Laws protecting intellectual property, such as patents, copyrights, and trade secrets, can be leveraged to file lawsuits against organizations that fail to protect these assets adequately. The legal ramifications can include both civil and criminal penalties, such as fines and, in extreme cases, imprisonment for key decision-makers within the organization.

Gaining unlawful access to computer systems can lead to criminal charges, often categorized under statutes like the Computer Fraud and Abuse Act (CFAA) in the United States. Such charges can result in imprisonment and hefty fines for individuals. The key element in such cases is the concept of "unauthorized access," which covers activities ranging from hacking into networks to merely exceeding the limits of authorized access.

ETHICS IN IS

Digital Privacy and Law Enforcement

A notable case that underscores the ethical dilemma faced by law enforcement regarding information security involves the FBI's handling of the iPhone belonging to one of the terrorists involved a December 2015 shooting in San Bernardino, CA. The FBI secured a court order requiring Apple to create a software bypass to the phone's encryption. Apple resisted,[16] sparking a national debate over the ethics of privacy and security. After Apple's refusal to create a bypass for the shooter's six-digit pin, the FBI found a small Australian company that had created an effective iPhone hacking tool that allowed them to break into the phone.[17] Although this meant that Apple was able to avoid creating a potentially dangerous tool that could compromise the safety and privacy of all Apple customers, there was one that already existed. The FBI was able to use this tool to work around the legal fight, but it did not resolve the ethical battle. The core of that ethical dilemma rested in balancing the need for national security and the investigation of a terrorist act against the protection of privacy rights and the potential implications of creating a vulnerability that could be exploited by others.

16 Tim Cook, "A Message to Our Customers," Apple, February 16, 2016, https://www.apple.com/customer-letter/
17 Adam Entous, "The FBI Wanted to Hack into the San Bernardino Shooter's iPhone. It Turned to a Little-Known Australian Firm," *Washington Post*, April 14, 2021, https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/

5.3 Information Security and Risk Management Strategies

Learning Objectives

By the end of this section, you will be able to:

- Identify the key components and principles of an effective ISRM strategy
- Describe various compliance frameworks and regulations related to information security and risk management and how they are used
- Develop a comprehensive risk management plan
- Determine the importance of continuous monitoring and improvement of the ISRM strategy

It is essential for today's organizations to have a well-crafted information security and risk management (ISRM) strategy, which is a structured approach to managing an organization's security processes, tools, and policies to mitigate risk. Organizations may be attracted to the capabilities of emerging technologies, but they must also recognize that it is imperative for them to safeguard their physical and digital assets. Not only does a well-structured ISRM strategy protect against data breaches and cyberattacks, it also serves as a mechanism for managing the organization's overall risk exposure.

Key Objectives, Principles, and Components of ISRM Strategy

ISRM does not merely involve deploying the latest security technologies or adhering to compliance regulations, although these are important. Its primary purpose is to develop a composed set of practices to protect an organization's informational assets and data infrastructure. A robust ISRM strategy aims to achieve three fundamental objectives: to safeguard organizational assets, to prevent data breaches and cyberattacks, and to reduce overall risk exposure. These objectives are embedded into the core components and principles that define the ideal ISRM strategy.

With cybercriminals employing increasingly sophisticated techniques, from social engineering to advanced malware, the need for proactive cyber defense mechanisms has also been increasing. These mechanisms should ideally include, but not be limited to, network monitoring, penetration testing, and employee training on cybersecurity best practices. A proactive approach can significantly reduce the probability of a successful attack, thereby preserving stakeholder trust and ensuring data integrity.

Another objective of ISRM is to reduce an organization's overall risk exposure. This involves not only implementing technological solutions, but also facilitating a cultural shift within the organization toward prioritizing cybersecurity. By conducting regular risk assessments, adopting a layered security approach, and encouraging a culture of cybersecurity awareness, organizations can significantly mitigate the risks they face. In doing so, organizations can protect their assets while simultaneously positioning themselves favorably in a competitive market where consumers and clients are becoming increasingly savvy about data security. To establish and maintain an effective ISRM strategy, several core components must be diligently addressed and continually refined. These include risk assessment, policy development, control implementation, training and awareness, monitoring and auditing, and response and recovery.

Risk Assessment

Risk assessment involves identifying potential threats and vulnerabilities, and the impact they could have on an organization's assets. It requires a thorough understanding of the organization's infrastructure, data, and business processes. By employing methodologies such as threat modeling and vulnerability assessments, organizations can prioritize risks based on their likelihood and potential impact, enabling them to allocate resources more effectively.

Policy Development

Policy development follows risk assessment as a critical step in articulating the organization's stance on various security issues. Policies provide a formal set of guidelines that dictate how assets should be protected and how security incidents should be managed. These policies should be clear, concise, and easily understandable, ensuring that all stakeholders, from the CEO to the newest employee, are on the same page regarding security expectations and responsibilities. Additionally, IT managers should ensure that the organization maintains adequate documentation such as acknowledgment forms and training records to track employee training.

Control Implementation

Control implementation involves putting into place the necessary safeguards to mitigate identified risks. These controls can be administrative (policies and procedures), technical (such as firewalls and encryption), or physical (like security cameras and access controls). The key is to establish a balanced mix of these controls to create a multilayered security environment. Control effectiveness should also be regularly reviewed to ensure they are performing as intended.

Training and Awareness

Training and awareness programs are essential for cultivating a culture of security within an organization. Employees are often the first line of defense against cyber threats, so it is vital that they are equipped with the knowledge and tools they need to recognize and respond to potential security incidents. Regular training sessions, coupled with awareness campaigns, can significantly reduce the risk of human error, which is a leading cause of data breaches.

Monitoring and Auditing

Monitoring and auditing are crucial for maintaining visibility over the organization's security posture. Continuous monitoring of network traffic, user activities, and system configurations ensures that any anomalous behavior can be detected and addressed promptly. Auditing provides a retrospective analysis, helping to uncover security lapses and ensure compliance with relevant laws and policies.

Response and Recovery

Finally, response and recovery involve being prepared to act when a security incident occurs. An organization should have in place a plan for **incident response**, which is a predetermined set of procedures and steps taken to identify, investigate, and respond to a potential security incident. After identifying the breach, an organization should have procedures for containing the threat, eradicating the malicious elements, and recovering any lost data. Post-incident analysis is also important, as it provides insights that can be used to strengthen the organization's defenses against future attacks.

By effectively addressing these core components, organizations can build a resilient ISRM strategy that can protect their assets, maintain stakeholder trust, and ensure the continuity of their operations. Each component is important, and only when they are seamlessly integrated can an organization truly safeguard itself in the digital age.

Compliance Frameworks and Regulations Related to ISRM

In the context of ISRM, a compliance framework is a set of guidelines and best practices designed to help an organization comply with legal, regulatory, and technical standards. It serves as the foundation of secure and resilient organizational practices. These frameworks provide a structured set of guidelines and best practices that are designed to aid organizations in safeguarding their digital assets and ensuring their adherence to the CIA triad. Additionally, these frameworks help to establish a foundation for security practices, aligning organizational processes with industry standards and thus ensuring legal and regulatory compliance.

For organizations aiming to support their security posture and maintain the trust of their stakeholders, adhering to regulations not only mitigates the risk of legal repercussions, but also fosters a culture of continuous improvement and due diligence in security practices.

Table 5.4 shows some of the frameworks that are often used to provide guidance for stakeholders as they seek to stay within the boundaries and laws of their organization's host government.

Framework	Description
ISO/IEC 27001 Information Security Management Systems Requirements	• International standard for ISRM • Provides a framework for constant improvement of an ISMS • Takes more of a risk-based approach to managing and securing sensitive information • Provides a structured methodology for compliance with best practices in information security
National Institute of Standards and Technology (NIST)	• Provides a framework for improving cybersecurity in multiple sectors • Flexible and adaptable to many fields • Consists of five core functions: identify, protect, detect, respond, and recover
NIST-800-137 NIST Special Publication 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"	• More specialized framework that provides comprehensive guidelines and best practices in cybersecurity • Provides detailed guidance on specific areas such as risk management, security controls, incident response, and information system security

Table 5.4 Common Frameworks Used in ISRM An organization may use multiple frameworks in developing a robust ISRM strategy.

ISO/IEC 27001

ISO/IEC 27001 is a globally recognized standard for the establishment and certification of an **information security management system (ISMS)**, a framework that helps organizations manage their information security by defining policies, procedures, and controls. Developed by the International Organization for Standardization (ISO), ISO/IEC 27001 sets out the criteria for assessing and treating information security risks tailored to the needs of the organization. The standard encompasses both the technical and organizational aspects of information security, ensuring an integrated approach.

The significance of ISO/IEC 27001 lies in its universal applicability across industries and organizations of any size. It provides a robust framework that helps organizations secure their information assets, enhance their resilience against cyber threats, and establish trust with stakeholders. By achieving certification, organizations demonstrate their commitment to information security, which can lead to competitive advantages, improved client relationships, and compliance with legal and regulatory requirements.

The ISO/IEC 27001 standard is structured into ten main clauses, with the last six dedicated to the ISMS requirements:[18]

1. Scope: Defines the boundaries and applicability of the ISMS
2. Normative references: Lists the standards referenced in ISO 27001

18 International Organization for Standardization, *ISO/IEC 27001:2022* (ISO, 2022).

3. Terms and definitions: Clarifies the terminology used in the standard
4. Context of the organization: Explains the internal and external factors that can impact the ISMS
5. Leadership: Emphasizes the importance of top management's involvement and the establishment of an information security policy
6. Planning: Covers risk assessment and the process of establishing information security objectives
7. Support: Encompasses resources, competence, awareness, communication, and documented information
8. Operation: Deals with the execution of the processes and controls necessary to manage information security risks
9. Performance evaluation: Involves monitoring, measurement, analysis, evaluation, internal audit, and management review
10. Improvement: Focuses on continual improvement of the ISMS

Although not one of the clauses, guidance on implementing specific controls is discussed in Annex A.

The principles of ISO/IEC 27001 are organized around a risk-based approach, and this ensures that the ISMS is tailored to the specific risks faced by the organization. The approach promotes a culture of continuous improvement, transparency, and accountability.

National Institute of Standards and Technology

Imagine taking the role as the new chief information security officer of a bank and the CEO asks you, "How secure are we?" How would you approach answering this question? Or where could you go to get the information? One place to start would be with the National Institute of Standards and Technology (NIST). NIST is a nonregulatory federal agency within the U.S. Department of Commerce that helps to set standards and guidelines to ensure the security and privacy of information systems. NIST's contribution to U.S. cybersecurity is significant, as the agency provides resources, best practices, and frameworks to assist organizations in safeguarding their information.

The NIST Special Publications 800 series is a collection of documents that cover various aspects of information security. These publications provide guidelines, recommendations, and best practices to help organizations manage and protect their information systems. Comparing the practices of your hypothetical bank against the guidelines set forth by NIST could help you answer your boss's question about security. One of the most notable contributions from NIST is the framework for improving critical infrastructure cybersecurity, commonly known as the NIST Cybersecurity Framework. This framework comprises five domains: identify, protect, detect, respond, and recover (refer to Figure 5.7). Each domain involves specific security activities that, when implemented, provide organizations with a strategic view of their cybersecurity posture.

Numerous organizations across different sectors have adopted NIST standards to enhance their cybersecurity practices. For example, a financial institution might align its security policies and procedures with NIST's best practices to improve its resilience against cyber threats. In the health-care sector, a hospital might use NIST guidelines to secure patient data and ensure HIPAA compliance. These real-world applications demonstrate the versatility and effectiveness of NIST standards in bolstering cybersecurity defenses and fostering a culture of security awareness and compliance.

Other Compliance Frameworks and Regulations

There are several frameworks and regulations in addition to NIST, NIST-800, and ISO/IEC 27001 that guide information security policy within an organization. Many of these depend on the nature of the business, the type of data that is collected, or even the geographic location of the business's headquarters.

- The Federal Information Security Management Act (FISMA) is a U.S. law that is part of the E-Government Act of 2002. It is designed to bolster information security across federal agencies, and it establishes a comprehensive framework that mandates agencies to develop, document, and implement security programs to protect information and assets. FISMA emphasizes a risk-based policy for cost-effective security, requiring agencies to conduct regular risk assessments, implement security measures, and undergo continuous monitoring. Compliance with FISMA demonstrates an organization's commitment to protecting governmental information and assets.

- The Health Information Technology for Economical and Clinical Health (HITECH) Act, enacted in 2009, represents significant legislation in health information technology and privacy. It aims to promote the adoption and meaningful use of health information technology, while also strengthening the privacy and security provisions of HIPAA. HITECH introduced stricter enforcement of HIPAA rules and increased penalties for noncompliance, emphasizing the need for health-care providers and related entities to safeguard electronic protected health information (ePHI). It also incentivized the implementation of electronic health records (EHRs), marking a transformative step in the modernization of health-care data management and security.

Developing a Comprehensive Risk Management Plan

A **risk management plan (RMP)** is a strategic document that outlines how risk is assessed, monitored, and mitigated within an organization. An RMP is a critical component in an organization's information security and risk management strategy. It provides a structured four-stage approach to identifying, assessing, mitigating, and monitoring potential risks that could compromise sensitive data, intellectual property, and other vital assets. This strategic document is crucial for shaping an organization's cybersecurity posture, guiding the allocation of resources, and prioritizing actions to enhance resilience against cyber threats.

Phase 1: Risk Identification

The initial phase of developing an RMP, identifying potential risks, is the priority. This process involves using various techniques and tools to uncover vulnerabilities, threats, and potential impact on organizational assets. A **strengths, weaknesses, opportunities, and threats (SWOT) analysis** is a commonly used method that helps in understanding both internal and external factors that could pose risks. When applied to risk identification in ISRM, SWOT becomes a powerful instrument in the hands of cybersecurity professionals. The SWOT analysis in Figure 5.10 shows how it has been used and adapted to meet the needs of a team assessing their own information security. By evaluating the strengths of an organization, such as robust security policies or advanced technological infrastructure, professionals can form policies that enhance brand value, increase employee awareness to reduce attacks, and make data-informed decisions regarding system upgrades.

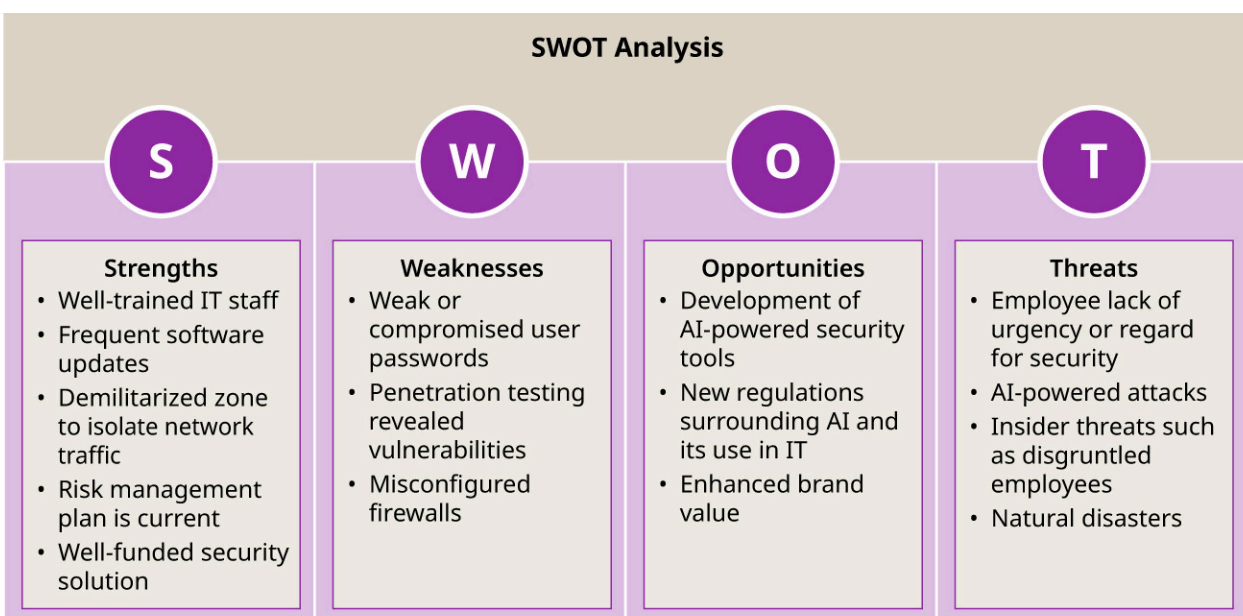


Figure 5.10 This hypothetical SWOT analysis completed by an information security team strategizes against threats to an IT system in a social media company. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The assets at risk in an organization can be vast and varied, including tangible assets such as hardware and intangible assets such as data and intellectual property. Protecting these assets requires a clear understanding of their value and the potential repercussions of any compromise. To aid in this process, a range of tools and technologies is available. Scanners, for instance, can automatically detect vulnerabilities in a network, while AI-based solutions offer advanced capabilities to predict and identify emerging threats. By employing these tools and methodologies, organizations can develop a clear and actionable understanding of their risk landscape, laying the foundation for effective risk management.

Phase 2: Risk Assessment

The risk assessment phase is a critical stage in the RMP, where the organization dives into the potential likelihood and impact of various identified risks. This process is like a detective's investigation, where each clue helps in prioritizing risks based on their severity. Imagine a team of cybersecurity experts evaluating a network system, much like detectives combing through a crime scene. They identify potential threats and vulnerabilities, such as what types of data are at risk, what protections are currently in place, and what additional measures are necessary to close any security gaps.

This phase is not just about finding problems, but also about devising strategies to mitigate them. Through risk assessments, ISRM professionals can make data-driven decisions to align security measures with organizational objectives. The comprehensive nature of risk assessment technologies and approaches highlights the need for ISRM professionals to have a similar breadth and depth of knowledge. With the appropriate certifications and continuous learning, these professionals can contribute to a safer and more secure digital landscape.

The two predominant assessment methods are quantitative and qualitative.

- Quantitative assessment: Quantitative assessments are often viewed as more time intensive than qualitative but can be more accurate when evaluating risk. The impact of the risk is often evaluated in the context of the expected cost of the risk. One method used in quantitative risk assessment is expected monetary value (EMV) analysis, which is a mathematical calculation for determining the expected monetary impact of risks: it multiplies the dollar cost of a risk by the probability of that risk occurring and then adds the values together for all risks. A decision tree analysis is another quantitative method that is more visual than EMV (Figure 5.11). The decision tree includes each risk, along with its financial impact and the probability associated with each risk. The project manager then can see the path that offers the least impact (cost) on the project. Regardless of the method chosen, quantitative risk assessment involves calculations that give a monetary value to the impact of the risks to the project.
- Qualitative assessment: Qualitative impacts can be categorized as high, medium, and low with the probability of occurrence ranked on a scale from very likely to highly unlikely. Even though the assessments are more subjective than the quantitative approaches, there are methods that can facilitate the processes. For example, a brainstorming session with key stakeholders or with the project team could generate a list of potential risks. Additionally, in-depth interviews with experts or stakeholders can identify risks and begin to assess the impact and probability. A SWOT analysis can be used as well. In particular, the internal weaknesses and the external threats can be considered risks to evaluate in the project.

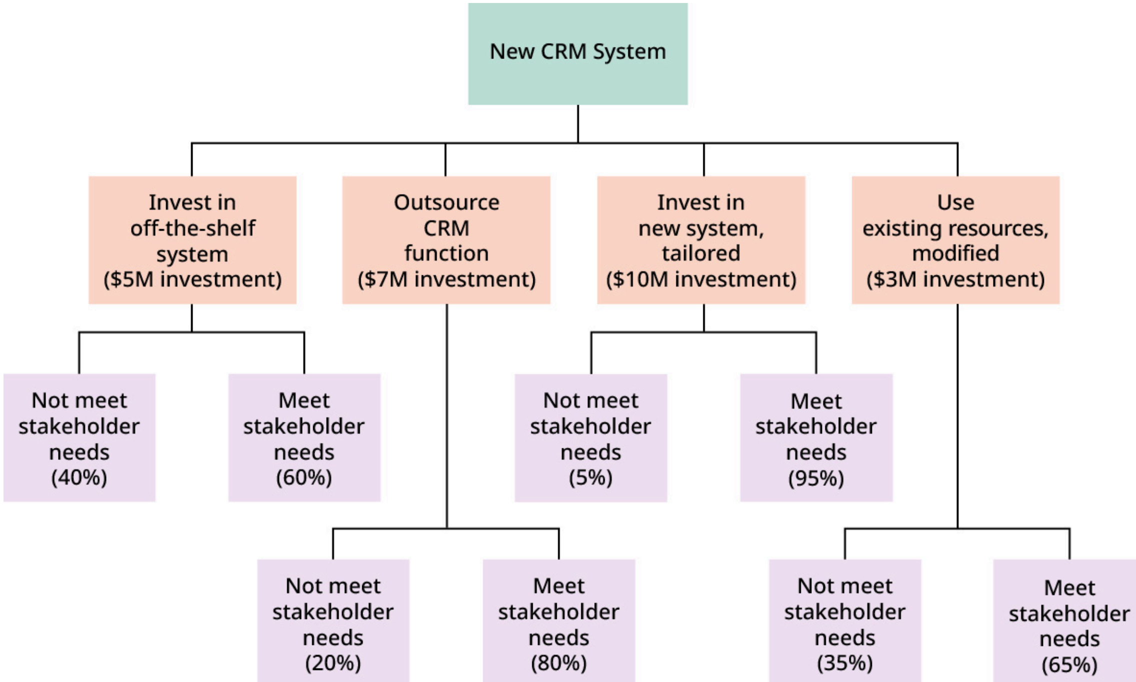


Figure 5.11 This hypothetical decision tree analysis shows how it can help a project manager visualize the various risks associated with a project. Through calculations such as EMV, the project manager can quantify the path that offers the least impact. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Another method used when conducting the qualitative assessment of risks is the Delphi method, which involves rounds of questionnaires sent to individuals with expertise who provide anonymous responses in which they identify risks and assess their impact and probabilities. The project manager will analyze the responses after each round to look for commonalities. Then, the compiled results are presented to the experts again and they have the opportunity reevaluate the responses and amend the list. The end result of the Delphi method is a list of risks that the experts have arrived at through this consensus-building process. Whatever method is used for conducting the qualitative assessment of the RMP, the important factor is to get input from various stakeholders and experts in the field to identify the risks and then organize the risks based on their impact and probability of occurrence. Figure 5.12 illustrates the contrast between quantitative and qualitative assessments when applied to an organization that specializes in IP generation.

Qualitative Assessment and Quantitative Assessment of Asset 1: Intellectual Property (IP)		**Qualitative Assessment and Quantitative Assessment of Asset 2: Human Resources (HR) Data**	
Qualitative Assessment	**Quantitative Assessment**	**Qualitative Assessment**	**Quantitative Assessment**
The loss or compromise of IP is categorized as high risk due to the potential severe impact on the company's competitive edge and market reputation. The likelihood of such an event could be rated as medium, considering the advanced security measures in place, yet acknowledging the high interest of competitors in this data.	If IP is compromised, the estimated financial loss is calculated at $5 million, considering factors like potential revenue loss, legal costs, and damages. The probability of this event, based on industry data and past incidents, is assessed at a 20% chance within the next year.	The breach of HR data, containing sensitive employee information, is categorized as medium risk. While it has significant implications for privacy and compliance (e.g., GDPR), it may not directly impact core business operations. The likelihood is assessed as high due to the larger volume of HR data and its accessibility.	A breach of HR data could lead to a financial impact of around $2 million, primarily due to legal repercussions and potential fines. The likelihood of such a breach is estimated at 30% in the next year, based on current trends in data breaches involving personal information.

Figure 5.12 This hypothetical scenario shows the two lenses of conducting a risk assessment: qualitative and quantitative. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

A risk matrix is a visual representation of the identified risks categorized by both impact and probability. A risk matrix can be used with both qualitative and quantitative assessments. In qualitative assessments, the matrix will be populated with categories that are subjective, such as high probability or low impact, whereas a quantitative risk matrix would include the numerical measures of these values. Often the matrix is color coded with a predetermined color scheme to help quickly identify those risks that have the highest impact or probability.

In Figure 5.13, the highest-risk items are highlighted in red with the lower-risk items in green. Each risk matrix can be evaluated by the project manager to determine which risks should be monitored more closely and to prioritize the highest impact items. Then, the RMP can address the appropriate risk mitigation strategies for those higher priority items while putting less focus on risks with minimal overall impact on the project.

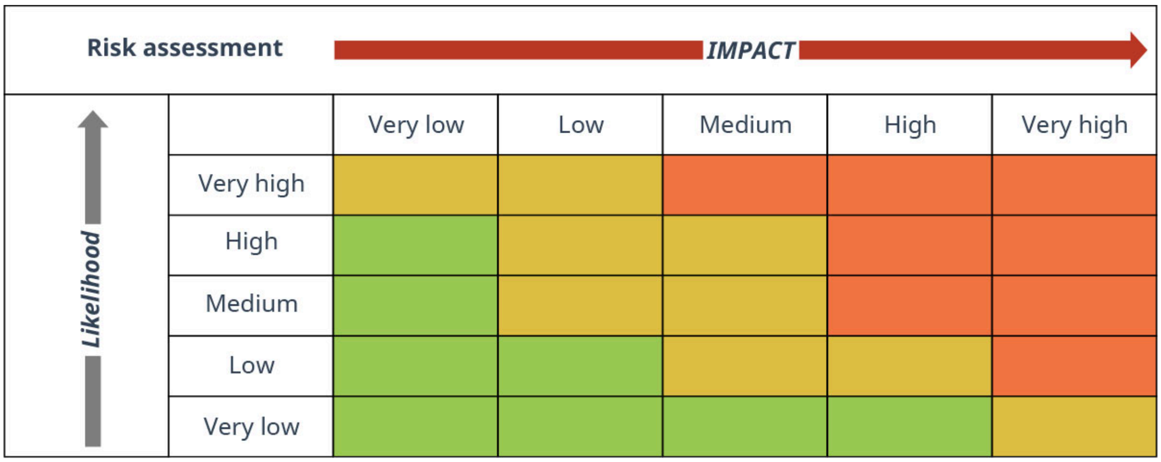


Figure 5.13 A risk matrix assists leaders in quantifying risks that may affect the organization. (credit: modification of work "Risk matrix (FAA Safety Risk Management Policy, 8040.4B)" by U.S. Department of Transportation Federal Aviation Administration/ Wikimedia Commons, Public Domain)

Phase 3: Risk Mitigation Strategies

Uncertainty in projects cannot be eliminated, but it can be mitigated. Some broad mitigation strategies include being proactive and developing a plan to deal with risks if they materialize. Each identified risk should have a strategy attached so that there is a plan in place to minimize the impact of the risk on the project. These broad strategies offer some general decisions that can be made with each risk; however, the actual activities used to alleviate the impact will need to be tailored to the specific risk. Figure 5.14 lists broad strategies for dealing with risk.

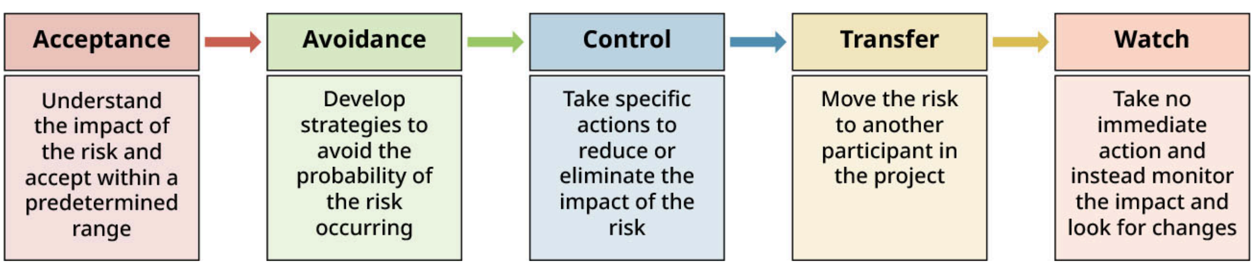


Figure 5.14 Developing action plans on how to deal with each risk in RMP can save time and money in the long run. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The first strategy, acceptance, describes a situation where the risk, impact, and probability are known, and the project team makes the decision to accept the impact. The risk might be at a level where it would not have a meaningful impact on the overall project. In some cases, the benefit of accepting the risk outweighs any negative impacts from the risk. Generally, the acceptance strategy is used when there are minimal impacts to the cost, the schedule, or team performance. It is important to continue to monitor the risk to ensure the impact remains at an acceptable level. Overall, the project continues to move forward without substantive consequences to the project plan and deliverables.

In the avoidance approach, the project team develops strategies to prevent the risk from occurring. For example, to avoid the risk of a new CRM system not functioning properly, the system could be tested with key stakeholders to make sure it meets performance measures. With risk avoidance, the project manager might consider moving resources from one part of the project (such as personnel or funding) to another part to help reduce the risk. Risk avoidance is used when there are risks to performance and could involve having backup vendors in case one vendor cannot fulfill what they are contracted to do. Avoiding risks to the schedule may involve setting realistic deadlines that are not too aggressive.

The control approach to mitigating risks involves trying to minimize the impact of risks. This involves consistent monitoring and having a plan in place to proactively respond to the risks. For example, tracking expenses against the expected budget at regular intervals can help the project team identify when line items are at risk of going over budget. When the project manager notices this, they can then implement strategies to manage the expense in that line to control the risk of going over budget. To control the risk of going over schedule, the project manager can keep close tabs on the time needed for tasks and redelegate as needed to make sure the project stays on time.

The transfer strategy can be used to shift the risk—and thus the impact—to another entity associated with the project. However, this approach may not be the best strategy because unintended consequences can arise. For example, if the project is running behind schedule, the project manager could transfer the cause of that delay to an individual team member rather than to the project team as a whole. Although the project team's reputation might be preserved somewhat, this kind of action could greatly impact the team dynamics. Likewise, if the impact of a product's failure is transferred to a particular vendor used to produce the product, the business relationship could be altered, even if the costs of the failure are no longer the responsibility of the project team. Caution should be used when choosing this strategy because of the additional consequences that could result.

Finally, the watch strategy involves essentially taking no action but having activities in place in the project plan to consistently monitor the risk for changes that could either increase the probability of occurrence or increase the impact. Strategies such as tracking the actual expenses versus budgeted expenses on a regular basis, or having project team updates on the status of action items, can be used to watch for changes. Monitoring is a key strategy that should be used for all risks identified and should be a key component of the RMP. The bottom line with any of the approaches to risk mitigation is to invest time on the front end of the planning process to be proactive in how the project team responds to risk.

Phase 4: Monitoring and Review

The implementation of risk mitigation strategies is not the end of the risk management process. In fact, mitigation requires ongoing attention and diligence to ensure its effectiveness and adaptability to new threats and changes in the organization's environment. This phase emphasizes the necessity of continuous monitoring and regular reviews to maintain the integrity of the RMP.

Frameworks for Continuous Monitoring and Improvement of the ISRM Strategy

The ongoing process of assessing the security posture and compliance of an IT infrastructure by automatically collecting, analyzing, and reporting data on various security controls is called **continuous monitoring**. It is critical for detecting and responding to threats and vulnerabilities in real time. It helps to ensure that the implemented risk mitigation strategies are working as intended and that no new risks have emerged. Continuous monitoring aids in maintaining a strong security posture, as it provides ongoing insights into the effectiveness of security controls and the organization's overall risk exposure.

Continuous monitoring plays an important role in ensuring the ongoing integrity, availability, and security of critical assets and information. Continuous monitoring is a necessary component of an effective ISRM strategy, ensuring that security controls are operating as intended and that any malicious activities are detected and addressed in a timely manner.

The **Information Systems Audit and Control Association (ISACA)** is an international association that provides IT professionals with knowledge, credentials, education, and community in IT governance, control, risk, security, audit, and assurance. IT governance is the process of managing and controlling an organization's IT capabilities to improve IT management, ensure compliance, and increase the value of IT investments. ISACA offers several certifications and comprehensive cyber education and plays an important role in setting global standards for cybersecurity. Through its publications, certifications, and guidance, ISACA provides industry best practices and frameworks that organizations can adopt to enhance their monitoring capabilities and align with relevant regulatory requirements.

One of ISACA's most notable contributions to the field is the development of the **Control Objectives for Information and Related Technologies (COBIT)** framework (Figure 5.15), a comprehensive framework developed by ISACA for IT governance and management that helps organizations meet business challenges in the areas of regulatory compliance, risk management, and aligning IT strategy with organizational goals.[19] In addition to COBIT5, NIST also provides a continuous monitoring strategy.[20] It is recognized globally and is widely adopted by organizations seeking to align their IT processes with their strategic objectives, while ensuring that risks are managed effectively and resources are used responsibly.

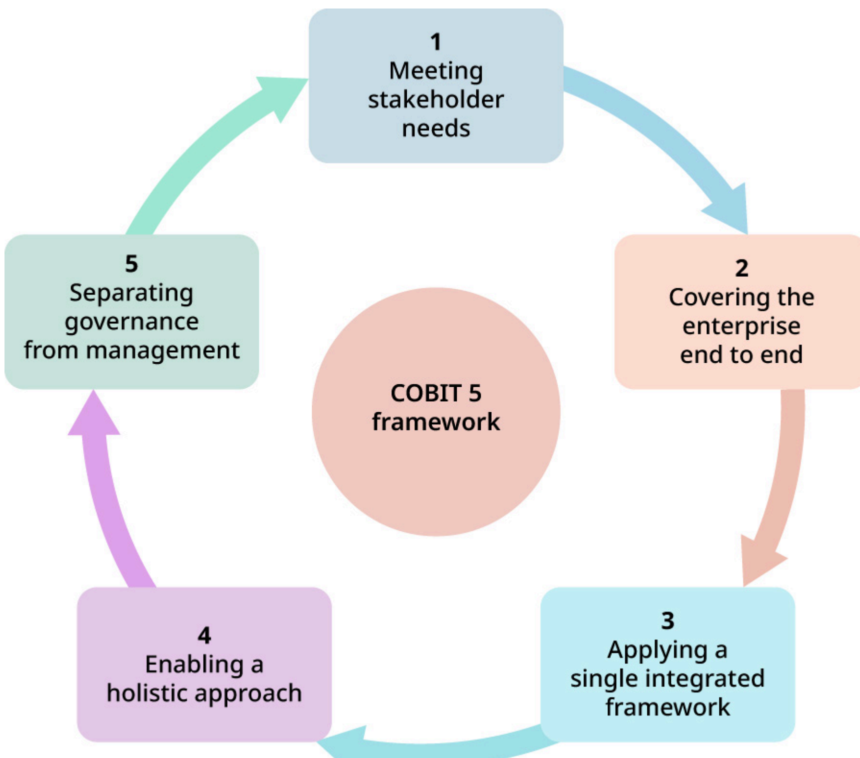


Figure 5.15 The COBIT5 framework consists of five principles that scaffold an IT governance structure. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Various tools and technologies play a pivotal role in facilitating continuous monitoring, each serving specific purposes and providing different insights into the organization's security posture.

One of the key tools available for continuous monitoring is a security information and event management (SIEM) system, a centralized security tool that combines security information management with security event

19 COBIT5 was published in 2012, and a new version (COBIT 2019) was released in 2018. COBIT 2019 was updated for newer technology and has six principles that use some revised terminology. Although COBIT 2019 is the most current version, many organizations still use COBIT5. 6.3 Data Security and Privacy from a Global Perspective discusses COBIT 2019.

20 Kelley Dempsey, Nirali S. Chawla, Arnold Johnson, et al. "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," *NIST Special Publication 800-137*, National Institute of Standards and Technology, September 2011, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

management. The tool collects, consolidates, and organizes data within the system, including user data, application data, and network data, to analyze and detect suspicious activity within the system. The aggregated data are analyzed to detect unusual activities, patterns, or events. The tools not only detect attacks but can also prevent and block threats to the system. Additionally, the tool can compile the necessary information for compliance reporting purposes. Finally, the SIEM system can monitor user actions to identify potential issues before those actions pose a threat to the organization. For example, if confidential employee information is being shared via email to an entity outside of the company that is not known to have a business need for the information, the SIEM system can flag those emails as threats. In a similar way, the system can identify incoming phishing emails and automatically block the sender. Through analytics, the SIEM system can quickly recognize unusual activity and take appropriate action to minimize the impact.

An intrusion detection system (IDS) is integrated into the SIEM system. The IDS looks specifically at traffic on the network to determine if there is suspicious activity coming into or out of the network. That data are then fed into the SIEM system to be aggregated with the other data gathered. The IDS can also detect security violations within the network. The tool does not stop the threat; it simply identifies the threat, sends the data on, and alerts network administrators of the threat. The IDS looks for known sources of threats. For example, the detection system could pick up on a specific chain of characters or source code that is part of a known malware threat. Because the IDS checks traffic against known threats, it is important to regularly update the system to make sure the newest cyber threats are being monitored.

The IDS works in conjunction with an intrusion prevention system (IPS) to prevent ongoing attacks to the network. The IPS is a more proactive approach to maintaining the security of the network. One example of an IPS is a firewall web application that prevents downloading of material from unsecured websites. To prevent threats from entering the network, all traffic goes through the IPS before entering the network. As with the IDS, the IPS works off of known threats, so new cyberattacks might get through. When suspicious activity is noticed, the IPS will block the activity from getting into the network, send an alert to administrators (facilitated by the SIEM system), and often terminate the connection where the threat originated in the system. This could mean a user is disconnected from the system to prevent further intrusion until the threat can be mitigated. Today’s IPS tools have detection capabilities built in and are now referred to as intrusion detection and prevention systems (IDPSs). Many organizations use one integrated tool rather than having two separate tools to manage security.

5.4 Career Focus: Key Certifications

Learning Objectives

By the end of this section, you will be able to:

- Describe various career roles and responsibilities in information security
- Determine the certifications and degree programs needed to prepare for a career in information security
- Recognize organizations where information security careers are most viable

At this point, you may be wondering how to find and obtain a job in one of the roles described in the information systems security field. The answer lies not just in building academic credentials, but also in gaining a variety of certifications. Obtaining a certification diversifies and deepens your expertise. These certifications demonstrate specialized knowledge and help individuals pursue career advancement.

The globally recognized Certified Information Systems Security Professional (CISSP) certification is one example. The CISSP and similar certifications enhance your skills and provide a mark of quality on your professional profile, making you a more desirable candidate in a competitive job market.

Information security is a sizable field that presents multiple pathways for career trajectories, each with its own challenges and rewards. From roles like a security analyst and network security engineer to high-level positions such as chief information security officer (CISO), the sector offers a spectrum of career avenues. The primary functions associated with these roles range from securing network perimeters to establishing organizational security strategies. It is essential to understand that certifications provide technical proficiency, but it is the alignment of this knowledge with specific job responsibilities that completes a person's professional portfolio.

Career Roles and Responsibilities in Information Security

With the rising complexities of information systems, there has been an increase in the number of roles that fall under the umbrella of information security. No longer is it a one-size-fits-all discipline that is solely the responsibility of an IT department. The field has morphed into a diverse landscape, offering an array of opportunities that encompass areas such as IT, business, law, and even psychology. From entry-level roles like security analysts to leadership positions such as CISOs, the profession now offers a variety of pathways for individuals with a range of interests and skills.

Overview of Information Security as a Profession

As you've learned, information security is the practice of safeguarding digital assets from unauthorized access, disclosure, alteration, or destruction. The scope of this profession has become both broad and deep, often encompassing multiple domains, including, but not limited to, network security, application security, endpoint security, identity management, cloud security, and even social engineering. In all these domains, the goal is still to protect an organization's data and systems from internal and external threats, thereby supporting its broader mission and objectives. In the public sector, it may involve safeguarding critical national infrastructure or sensitive governmental data.

LINK TO LEARNING

As a cybersecurity professional, it is vitally important to stay up to date with the latest developments in cybersecurity. This field changes often as new technologies are developed and hackers develop new methods of attack. SANS provides a variety of free and paid information security resources (https://openstax.org/r/109SecResources) such as courses, conferences, and newsletters.

The field of information security straddles several disciplines, and professionals may be able to integrate knowledge and techniques from a variety of sectors. While not an exhaustive list, Table 5.5 identifies some of these disciplines that intersect within the information security field.

Discipline	Relation to Information Security
Information technology	IT forms the backbone of information security. Professionals need to be familiar with various hardware and software systems, network protocols, and security architectures.
Business	Understanding the strategic goals and operational nuances of an organization is key to effective security planning. It includes concepts such as business continuity and disaster recovery planning.
Law	Legal considerations, such as compliance with regulations like HIPAA in U.S. health care or GDPR in the European Union, are fundamental. Ignorance of legal requirements is not an excuse, and the ramifications of noncompliance can be severe.

Table 5.5 Disciplines within the Information Security Field Information systems is an eclectic discipline with several connected disciplines.

Discipline	Relation to Information Security
Psychology	An often-overlooked aspect of information security is understanding human behavior, especially as it relates to social engineering tactics. Security awareness training, for instance, is an important element for creating a secure organization.
Ethics	The ethical dimensions of data management and privacy are increasingly gaining prominence, especially as society becomes more conscious of individual rights related to personal data.

Table 5.5 Disciplines within the Information Security Field Information systems is an eclectic discipline with several connected disciplines.

Roles and Careers in Information Security

A career in information security not only requires a good understanding of technology, but it also requires a holistic understanding of a variety of subjects that impact the security of an organization. By acknowledging this interdisciplinary nature, professionals can better position themselves for successful and impactful careers. Roles in cybersecurity fields range from those working in a security operations center to specialized positions such as cryptographers and forensic specialists, as noted in Table 5.6.

Field	Role
Security operations center	The security analyst typically serves as an organization's first line of defense, monitoring security alerts, analyzing anomalies, and initiating incident response protocols. Their role may also include vulnerability assessment and working with different departments to improve overall security posture.
Security governance and risk	Security governance and risk roles represent a merger between the duties of a security auditor and a security engineer.
Strategic security management	Typically, an information security manager is responsible for the day-to-day operations related to cybersecurity. This could include overseeing a team of security experts, managing security initiatives, and ensuring compliance with internal and external regulations.
Forensics and ethics	Forensic experts specialize in investigating and analyzing past security incidents to understand how they occurred and to recommend ways to prevent future occurrences. They are the detectives of the cyber world, piecing together clues to resolve complex security puzzles.

Table 5.6 Roles in Cybersecurity Fields There are various career opportunities in the information systems security and risk management domains.

Together, these roles create a robust framework for both proactive and reactive security measures, encompassing the creation of secure environments, detailed investigation of breaches, and preemptive identification of potential vulnerabilities. This consolidated specialization serves as an advanced line of defense, often working behind the scenes, that is critically important in bolstering an organization's overall cybersecurity posture.

LINK TO LEARNING

The Information Security Forum is a professional organization that provides links to security research (https://openstax.org/r/109SecResearch) as well as forums, tools, products, services, events, and news regarding information security and risk management.

Certifications and Degree Programs for Careers in Information Security

Continuous professional development is fundamental in information security. As threats become more sophisticated and bad actors continue to refine their craft, ongoing education is necessary. Within this context, certifications and formal education programs serve dual purposes. First, they provide the foundational and advanced knowledge required to confront emerging security challenges effectively. Second, they serve as universally recognized markers of expertise, enhancing career prospects and lending credibility to skills.

The role of certifications in information security is important. A certification such as **Certified Ethical Hacker (CEH)** signifies proficiency in ethical hacking techniques and tools, and the ability to assess the security of computer systems by looking for vulnerabilities in a lawful and legitimate manner. CompTIA is a professional organization that specializes in certifications in IT. **Security+** is an entry-level certification from CompTIA that covers foundational skills and knowledge in network security, compliance, operational security, threats and vulnerabilities, data and host security, access control, and identity management. Other certifications offer structured learning paths and are often prerequisites for specialized roles in the industry (Table 5.7). For example, **Certified Information Security Manager (CISM)** focuses on management and governance of information security, and **Certified Information Systems Security Professional (CISSP)** is an advanced certification that focuses on the knowledge and skills required to design, implement, and manage a comprehensive information security program. Certifications act as both a road map for skill acquisition and a validation of those skills, especially valuable for professionals looking to transition into higher-level positions.

Certification	Related Jobs
CompTIA A+	Systems administrator, help desk technician, computer repair specialist, desktop support technician, IT asset manager, field service technician
CompTIA Security+	Security administrator, security analyst, incident response analyst, cybersecurity analyst
Cisco Certified Network Professional	Network engineer, network administrator, cloud network engineer, solutions architect, IT manager
EC-Council Certified Ethical Hacker	Cybercrime investigator, ethical hacker, forensic investigator, penetration tester, information security auditor, vulnerability analyst
Certified Information Systems Security Professional (CISSP)	Chief information security officer (CISO), incident response manager, cybersecurity engineer, risk manager, security analyst

Table 5.7 Common Certifications and Related Jobs There are several certifications available for those looking to work in a cyber-related field.

Formal education, such as bachelor's and master's degrees in cybersecurity or information security, provides a comprehensive overview of the field. These programs often cover a broader curriculum, touching on related disciplines such as business, law, and ethics, preparing students for the interdisciplinary nature of modern information security roles.

Both certifications and formal degree programs are vital in shaping a path to a successful career in information security. They equip professionals with the skills needed to adapt and thrive in a dynamic environment while simultaneously serving as benchmarks of competence for employers.

Empowering Cybersecurity Careers: Value and Impact of Professional Certifications and Related Degrees

Certifications and degrees in information security play an important role in validating a professional's skills and competencies. While traditional degree programs offer a broad scope of knowledge, certifications are focused on skill sets and methodologies directly applicable to the job. Unlike generic evaluations or internal assessments within an organization, certifications are designed and recognized by industry experts. Obtaining a certification often requires passing rigorous exams and, in some instances, demonstrating hands-on expertise in a controlled environment. As such, certifications act as a third-party endorsement of a professional's capabilities, lending weight to résumés and professional profiles.

Certifications

CEH certification concentrates on penetration testing and vulnerability assessments, skills immediately deployable in the workplace. Cisco's Certified Network Professional (CCNP), which focuses on advanced networking practices, is highly sought after by employers looking to increase their talent pool. Selecting the right certifications is a foundational step for a strong and definitive career path in information security. Certifications signal to employers that a candidate possesses a level of technical insight that has been rigorously evaluated and approved by a recognized accrediting body. In an increasingly competitive job market, such validation can distinguish one individual from other professionals in the field, and in many cases, it may be a formal requirement for securing a particular role.

Each certification level, whether entry-level or advanced, typically builds on the last, creating a pathway for continuous skill acquisition and career progression. This is particularly significant in information security. By regularly updating and expanding your certification portfolio, you are not just meeting the requirements of your current role, but also preparing yourself for the more complex challenges that lie ahead in higher-level positions.

For example, suppose you are an IT professional with experience in data analysis, and you are interested in transitioning into a threat intelligence analyst role. In this case, CompTIA Cybersecurity Analyst (CySA+) would be a strategic certification to pursue. The CySA+ specializes in behavioral analytics to identify cybersecurity threats, a skill often required for threat intelligence analysis. For more senior roles, such as information security manager or CISO, the CISSP is considered a gold standard. The CISSP provides a comprehensive overview of information security and may be a requirement for high-level security roles within large organizations.

Aligning certifications with career goals can deliver tangible benefits, enabling individuals to tailor their professional development to meet the expectations of future roles. It is worth investing the time to research and select the certifications that offer the most direct path toward a desired career trajectory in the field of information security.

Degree Programs

Earning certifications in cybersecurity-related fields can help with obtaining employment with many employers. However, degree programs complement the certification stack and demonstrate to potential employers that you can perform tasks both in an academic and in a technical manner. Additionally, many employers seek individuals who possess a degree in higher education for higher level roles in an organization such as chief information officer or CISO. For example, in their analysis of employer hiring behaviors, one study found that several employers favored those who possessed a degree accompanied by certifications over those with certifications alone (Figure 5.16).[21]

Figure 5.16 Obtaining a degree in a cyber-related field greatly improves your chances of employment. (credit: modification of work "Spring 2023 commencement ceremony" by Germanna Community College/Flickr, CC BY 2.0)

Degrees in cyber-related fields include the following:

- Undergraduate programs: Bachelor in cybersecurity. Many institutions offer a bachelor's degree in a cybersecurity-related discipline. Several of these programs incorporate general networking, ethical hacking, penetration testing, programming in various languages (such as Python, C#, and C++), and network defense. Additionally, these programs often have specializations or "tracks" that allow students to specialize in a particular area of cybersecurity. According to the U.S. Bureau of Statistics, the number of jobs related to cybersecurity to be added by the year 2033 could be more than 59,000.[22] Many of these positions require a minimum of a bachelor's degree coupled with certifications to be considered for employment.
- Graduate programs: Master in cybersecurity. Those holding this credential are often sought after by enterprise organizations looking to hire senior-level managers to oversee teams in a cybersecurity environment. Those enrolled in these programs acquire industry-recognized skills along with skills in leadership and management. The curriculum in these programs is normally designed to expose learners to practical skills that can be immediately applied upon graduation.

Combining Certifications and Degrees

Combining both certifications and formal education provides the benefits of a formal degree coupled with industry-recognized skill sets. Formal education helps to provide a broad theoretical understanding of the field along with the soft skills sought after by the industry. Moreover, the depth of knowledge gained during the formal education process helps to reinforce the concepts of practical application by supplying a broad understanding of the field.

21 Jim Marquardson and Ahmed Elnoshokaty, "Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs," *Information Systems Education Journal* 18, no. 1 (2020): 22–28.
22 Bureau of Labor Statistics, "Information Security Analysts," *Occupational Outlook Handbook*, U.S. Department of Labor, last modified August 29, 2024, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

The act of acquiring both industry-recognized certifications and formal educational qualifications in cybersecurity demonstrates more than mere skill acquisition; it reflects a commitment to mastering the complexities of the field. Each of these educational pathways offers benefits. Certifications such as Security+, CISSP, or CISM are tailored to validate a specific set of skills and are often updated more frequently than traditional academic curricula. They provide practical, firsthand experience and are excellent at helping to build immediate competency in specialized areas. Certifications also offer quicker routes to career advancement by serving as easily recognizable benchmarks for employers.

Organizations for Information Security Careers

A fulfilling career in the cybersecurity domain depends not only on skill and qualifications, but also on the organization one joins. Organizations provide context in which professionals apply their expertise to real-world challenges, influencing both job satisfaction and career path. Therefore, selecting the right workplace becomes an important decision, affecting not just individual career growth, but also the broader mission of enhancing digital trust in society.

Corporate Sector

The corporate sector is the most expansive area for information security professionals, encompassing technology companies, financial institutions, health-care providers, and e-commerce businesses. Each of these subsectors demands specialized knowledge and skill sets, from safeguarding intellectual property to ensuring customer data privacy.

FUTURE TECHNOLOGY

Meta's AI

After the release of ChatGPT from Open AI, several tech companies rushed to develop their own models to compete. For example, Google developed Bard (now known as Gemini), Tesla is working on their own models under xAI to try to generate a platform that outperforms GPT, and Microsoft implemented Copilot, which is another large language model (LLM) that was deployed in November 2023. Another contender in this field is Meta, who released the second iteration of their open-source LLM called Llama 2 in 2023. Their model is optimized for lower resource usage and can be deployed in a number of environments, ranging from academia to the commercial sector. One other important feature of the Llama 2 model is its ability to be trained and adapted to complete different tasks. Meta has partnered with Microsoft for Llama 2 to provide global access to their AI technology to encourage users to innovate by building on their model, which can in turn benefit businesses around the world.

Government, Public Sector, and Nonprofit Think Tanks

In the government and public sector, certified information security professionals contribute significantly to the safeguarding of national interests and public welfare. Holding certifications not only validates a professional's skills, but also reinforces the level of trust and credibility in governmental operations. For example, certified professionals can be instrumental in developing secure electoral systems, safeguarding public health records, and ensuring the confidentiality of sensitive diplomatic communications. By doing so, they facilitate an environment of digital trust that is important to maintain the public's confidence in governmental systems and operations. Professionals in this area are often employed by government agencies such as the Department of Defense or the Department of Justice.

The nonprofit sector and think tanks also help to shape the landscape of information security. These organizations primarily focus on research, advocacy, and public awareness, often working to address the cybersecurity needs of vulnerable populations or to shape public policy. They apply their specialized knowledge to developing solutions or frameworks that advance the cause of digital trust. Certified professionals may be seen as holders of digital trust, advocating for responsible and secure use of technology. Some of these types of entities include:

- Cybersecurity research organizations: Nonprofits such as the Electronic Frontier Foundation (EFF) or the Center for Internet Security (CIS) often conduct groundbreaking research on cyber threats, security technologies, and ethical computing practices. Their work may result in white papers, open-source tools, or policy recommendations.
- Educational institutions: Think tanks and educational nonprofits aim to raise cybersecurity awareness and literacy. They may offer training programs, certifications, or collaborate with academic institutions to promote cybersecurity as an essential part of the curriculum.

Freelance and Consultancy

The freelance and consultancy sector is suitable for those who prefer project-based or contractual work, often serving clients across the same sectors. It offers flexibility but demands a versatile skill set and an entrepreneurial mindset. In any of these sectors, certifications serve as a testament to an individual's skills and as a basis for advancing digital trust. A certified professional lends credibility to an organization's cybersecurity posture, thereby facilitating trust.

LINK TO LEARNING

There are many opportunities available to those interested in freelancing or performing consulting work in cybersecurity. Some of these resources include online courses, industry forums, and professional networks. Read this article about becoming a cybersecurity consultant (https://openstax.org/r/109CyberConsult) from Springboard for some suggestions on getting started.

Importance of Continuous Learning and Adaptability

Cybersecurity is a rapidly changing field with evolving threats and vulnerabilities that demand constant vigilance. Herein lies the importance of continuous learning and adaptability. The ongoing process of acquiring new knowledge and skills, particularly to keep pace with evolving cybersecurity threats and technologies, is called continuous learning. The ability to change or be changed to fit new circumstances is called adaptability, which is a critical trait for cybersecurity professionals facing a dynamic threat landscape. Cyber threats mutate and adapt, and so must professionals in the field.

Technologies such as cloud computing and generative AI bring novel challenges, such as data breaches and AI-powered attacks. These evolving risks highlight the importance of adaptability and continuous learning in cybersecurity. Staying informed and flexible enables professionals to effectively safeguard digital trust across all sectors. Additionally, the ability to pivot and evolve your skill set in response to new types of cybersecurity risks is invaluable. It is this combination of continuous learning and adaptability that enables an information security professional to remain effective.

LINK TO LEARNING

As more nations adopt AI, there encounter both benefits and risks. On one hand, AI can be leveraged to read x-rays, and chat with a person in real time, or complete mundane tasks. On the other hand, AI can also be used to ramp up social engineering attacks (https://openstax.org/r/109AIAttacks) such as phishing, spam, and other malicious applications that threaten security.

Key Terms

advanced encryption standard (AES) symmetric encryption algorithm used globally to secure data, known for its speed and security

artificial intelligence (AI) branch of computer science focused on creating intelligent machines capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation

asymmetric encryption (also, public-key cryptography) type of encryption that uses a public and private key

authentication process of verifying the identity of a user or device, often through credentials such as passwords or digital certificates

brute-force attack attack method where an attacker systematically checks all password or encryption key possibilities until the correct one is found

buffer overflow condition where an application writes more data to a buffer than it can hold

Certified Ethical Hacker (CEH) certification that signifies proficiency in ethical hacking techniques and tools, and the ability to assess the security of computer systems by looking for vulnerabilities in a lawful and legitimate manner

Certified Information Security Manager (CISM) certification that focuses on management and governance of information security

Certified Information Systems Security Professional (CISSP) advanced certification that focuses on the knowledge and skills required to design, implement, and manage a comprehensive information security program

classless inter-domain routing (CIDR) method for allocating IP addresses and routing IP packets more efficiently than traditional classful IP addressing

confidentiality, integrity, availability (CIA) triad foundational model in cybersecurity that ensures information is protected, accurate and trustworthy, and readily available to authorized users

continuous monitoring ongoing process of assessing the security posture and compliance of an IT infrastructure by automatically collecting, analyzing, and reporting data on various security controls

Control Objectives for Information and Related Technologies (COBIT5) framework comprehensive framework developed by ISACA for IT governance and management that helps organizations meet business challenges in the areas of regulatory compliance, risk management, and aligning IT strategy with organizational goals

cryptographic key string of data used by encryption algorithms to transform data into a secure format and its subsequent decryption

cybersecurity practice of protecting systems, networks, devices, and data from online threats

data packet small unit of data transmitted over a network

dictionary attack attack method where an attacker uses a precompiled list of likely passwords

digital signature electronic signature that uses cryptographic techniques to provide authentication and ensure the integrity of the signed digital document or message

distributed denial-of-service (DDoS) attack that uses multiple computers or servers to overwhelm a network resulting in loss of usability

Domain Name System (DNS) system that translates human-readable domain names to IP addresses, allowing users to access websites using familiar names

dynamic IP address address that is assigned each time a device connects to the internet; changes periodically, although not necessarily every time the device connects

encryption process of transforming legible data into a coded format, making it unreadable to unauthorized entities

environmental threat uncontrollable external factor such as a natural disaster or hardware failure that can damage data centers and disrupt business operations

ethical hacking process of attempting to break into an organization's computer systems, network, or applications with permission to identify vulnerabilities

external threat threat that originates from outside an organization, typically posed by cybercriminals or state-sponsored attackers who aim to exploit vulnerabilities for financial or strategic gain
fileless malware type of malware that exploits in-memory processes to conduct its nefarious activities
firewall network security system that uses security rules to monitor and control incoming and outgoing traffic
hashing process of converting data into a fixed-size string of characters, typically used for security purposes to ensure data integrity
HTTP Secure (HTTPS) protocol that adds a secure, encrypted layer to HTTP via SSL/TLS protocols
Hypertext Transfer Protocol (HTTP) protocol that is proficient at transmitting hypertext over the internet
incident response predetermined set of procedures and steps taken to identify, investigate, and respond to potential security incidents
information privacy right and measure of control individuals have over the collection, storage, management, and dissemination of their personal information
information security practice of protecting information by mitigating information risks and vulnerabilities, which encompasses data privacy, data confidentiality, data integrity, and data availability; employs methods such as encryption, firewalls, and secure network design
information security management system (ISMS) framework that helps organizations manage their information security by defining policies, procedures, and controls
information security risk management (ISRM) field that involves identifying, assessing, and mitigating risks to the confidentiality, integrity, and availability of information and information systems
Information Systems Audit and Control Association (ISACA) international association that provides IT professionals with knowledge, credentials, education, and community in IT governance, control, risk, security, audit, and assurance
intellectual property (IP) creations of the mind that are protected by law from unauthorized use or replication
internal threat one that originates from within an organization, such as disgruntled employees or poor security training for employees resulting in social engineering attacks
internet protocol (IP) address unique identifier that allows a computer to be addressed in order to communicate on the internet
Internet Protocol Security (IPsec) suite of protocols that provides end-to-end encryption and secure data exchange
intrusion detection and prevention system (IDPS) tool that monitors networks for malicious activity or policy violations
IT governance process of managing and controlling an organization’s IT capabilities to improve IT management, ensure compliance, and increase the value of IT investments
keylogger tool or technology often used maliciously to capture keystrokes on a computer to obtain sensitive information such as passwords
log file file generated by security applications that contains event information that aids in determining the status and health of a network
malware malicious software designed to damage, exploit, infect systems, or otherwise compromise data, devices, users, or networks, using viruses, worms, and spyware that is installed into the basic input-output system (BIOS) of a computer
media access control (MAC) address unique identifier that allows a computer to be addressed in order to communicate within a local area network
multi factor authentication (MFA) security measure that requires users to verify their identity using multiple forms of credentials, such as a password, a security token, or biometric data, to access a system
network security process of guarding network infrastructure and IT systems from unauthorized access, misuse, malfunction, or improper disclosure to unintended parties
packet sniffer (also, network analyzer or protocol analyzer) tool that captures and analyzes network traffic
phishing type of social engineering attack that appears as a trustworthy entity in digital communication but

steals user data, such as login credentials and financial information

pretexting social engineering attack that involves creating a fabricated scenario to obtain private data

protocol fundamental rule or procedure that governs communication between devices in a network

protocol analyzer tool that examines network communication protocols to understand how data are exchanged between devices and applications on a network

ransomware type of malicious software that encrypts users' files such as photos, documents, or other sensitive information and demands a ransom for their release

risk appetite level of risk an organization is willing to accept in pursuit of its ambitions or goals

risk management plan (RMP) strategic document that outlines how risk is assessed, monitored, and mitigated within an organization

risk tolerance number of unfavorable outcomes an organization is willing to accept while pursuing goals and other objectives

role-based access control (RBAC) method of access control that bases data access on a person's role in the organization, giving each employee the minimum level of access they need to perform their job functions

rootkit software that enables attackers to have access to a system masquerading as operating system processes

router device that forwards data packets to the appropriate parts of a computer network

RSA encryption asymmetric cryptographic algorithm used for secure data transmission; particularly useful in public-key cryptography

Secure Sockets Layer (SSL) communication protocol that establishes a secure connection between devices or applications on a network by encrypting data sent between a browser and a website or between two servers

security information and event management (SIEM) security solution that collects, analyzes, and correlates security data from different sources to detect and respond to security threats in real time

Security+ entry-level certification that covers foundational skills and knowledge in network security, compliance, operational security, threats and vulnerabilities, data and host security, access control, and identity management

server powerful computer or computer program that provides data to other computers (clients) over a network

social engineering manipulation of employees into revealing sensitive information, often leading to unauthorized system access

static IP address permanent address assigned by an administrator that remains the same over time and is essential for services such as hosting servers, email servers, and network devices, or when remote access is required

strengths, weaknesses, opportunities, and threats (SWOT) analysis commonly used method that helps in understanding both internal and external factors that could pose risks

subnet logically visible subdivision of an IP network, increasing its efficiency and security

subnet mask address used in routing and network organization that divides the IP address into network and host addresses

switch device that connects and segments various components within a local network

symmetric encryption type of encryption in which one key both encrypts and decrypts the data

Transport Layer Security (TLS) updated version of SSL that uses an encrypted tunnel to protect data sent between a browser, a website, and the website's server

Trojan program that conceals itself as a safe program but often carries many other different types of malicious payloads

virtual private network (VPN) service that creates a secure, encrypted connection over a less secure network, typically the internet, ensuring private data remains protected

virus malware that attaches itself to clean files and propagate to other files and programs

worm stand-alone software program that spreads without requiring a host program

Summary

5.1 The Importance of Network Security

- Routers act as gateways to both internal and external networks, with the capability of blocking unauthorized access and filtering traffic when the router has a firewall installed in it.
- Switches allow for network segmentation, and they can provide another layer of security by isolating traffic within VLANs.
- Networks go far beyond basic components and include protocols and services that control how information is transmitted and received. These items may include advanced firewalls, intrusion detection systems, and intrusion prevention systems.
- Key principles of network security include confidentiality, integrity, and availability (CIA) along with ensuring authentication, and authorization to track and monitor access.
- Information security focuses on shielding information from unauthorized access and breaches, promoting confidentiality, integrity, and availability of data. Alternatively, information privacy involves the proper handling, use, and storage of information and focuses more on the rights of individuals.
- There are several types of data that range broadly from simple files such as text messages, videos, and pictures to more sensitive types of data such as passwords, intellectual property, and personal data that require special handling and storage to promote safety.
- Vulnerabilities range widely from poorly configured networks to poorly trained staff weak in areas such as social engineering.

5.2 Security Technologies and Solutions

- Robust antivirus, anti-malware solutions, and intrusion detection systems are foundational technologies and solutions critical for protecting information and networks against a multitude of cyber threats.
- Understanding the nature of malware, social engineering, insider threats, DDoS attacks, and software and hardware vulnerabilities enables the identification of potential security threats and the selection of targeted countermeasures such as employee training and regular software patching.
- Regular penetration testing and vulnerability assessments are vital in recognizing security flaws, allowing for the proactive remediation of threats and the reinforcement of an organization’s cyber defenses.
- Secure computing and risk management best practices involve conducting regular security assessments and enforcing access control policies to safeguard organizational assets effectively.
- While the cyber domain may be vast, there are several regulatory frameworks, such as GDPR and CCPA that provide protection for consumers from data mishandling, theft, and exploitation.
- Ethical considerations in cybersecurity, such as those involving ethical hacking, demonstrate the importance of employing security skills for defensive purposes, supported by a strict code of ethics to prevent misuse of expertise.

5.3 Information Security and Risk Management Strategies

- An effective ISRM strategy integrates risk identification, protection mechanisms, incident response, and recovery strategies, and it is underpinned by continuous monitoring and improvement.
- A comprehensive risk management plan encompasses the identification of potential threats, assessment of vulnerabilities, implementation of protective controls, and continuous evaluation to mitigate risks to the organization’s information assets.
- Compliance frameworks such as COBIT5 by ISACA and regulations such as NIST’s standards provide structured guidelines and best practices that organizations can use to align their ISRM strategies with industry requirements and improve their security posture.
- Continuous monitoring and improvement are vital to an organization’s ISRM strategy, ensuring that the organization can adapt to new threats, leverage emerging technologies, and refine defenses in line with the changing security landscape.

5.4 Career Focus: Key Certifications

- The chief information security officer (CISO) oversees an organization's overall security strategy, developing policies and managing the protection of IT infrastructure, including incident response planning.
- Information security is an interdisciplinary field involving several sectors, such as IT, business, law, and psychology. This combination of disciplines is driven by the evolving nature of cyber threats and requires IT security professionals to be highly adaptable or have knowledge that spans several domains of IT.
- Earning certifications validates a professional's expertise and dedication to the field of cybersecurity. These certifications can be pivotal for career progression, moving professionals into specialized roles or leadership positions within information security.
- While entry-level certifications provide foundational knowledge, advanced certifications and degrees demonstrate a candidate's broad and deep knowledge of information security as well as their suitability for taking on high-level managerial roles that involve overseeing an organization's security strategy and IT teams. Financial institutions, government agencies, and health-care organizations are highly viable sectors for information security careers due to their need to protect sensitive data, comply with stringent regulations, and maintain public trust.
- Cybersecurity careers are not limited to the IT industry; they are critical in diverse sectors such as manufacturing, retail, and education. This is due to the increasing reliance on digital systems and the imperative to protect against growing cybersecurity threats in all areas of commerce and society.

Review Questions

1. What principle primarily concerns protecting information from unauthorized access, modification, or deletion?
   a. data encryption
   b. information security
   c. information privacy
   d. user authentication

2. What type of attack manipulates the Domain Name System (DNS) to redirect a website's traffic to a different IP address?
   a. phishing
   b. spoofing
   c. man-in-the-middle
   d. brute-force attack

3. What type of social engineering attack appears as a trustworthy entity in digital communication but steals user data, such as login credentials and financial information?
   a. spoofing
   b. hacking
   c. identity theft
   d. phishing

4. What authentication mechanism is the most secure?
   a. username and password
   b. two-factor authentication
   c. multi factor authentication
   d. biometric verification

5. What is the purpose of role-based access control (RBAC) in network security?
   a. to monitor and filter outgoing internet traffic
   b. to prevent data loss through email and web applications

   c. to ensure users have access only to the resources necessary for their roles
   d. to encrypt data transmissions over the network

6. Why are regular penetration tests important for maintaining organizational security?
   a. They help in training IT staff on how to respond to media inquiries.
   b. They allow for constant updating of the company website's content.
   c. They enable the identification and remediation of early vulnerabilities.
   d. They are a regulatory requirement for all businesses.

7. What is the cyber safety significance of applying regular software updates and patches?
   a. They maintain the software's compatibility with new hardware.
   b. They often add new features to the software.
   c. They address identified security vulnerabilities to prevent exploits.
   d. They are mainly for aesthetic improvements to the user interface.

8. How does ethical hacking differ from malicious hacking?
   a. Ethical hacking is performed without the permission of the target entity.
   b. Ethical hacking is intended to strengthen systems, not to harm them.
   c. Ethical hacking does not require a deep understanding of IT systems.
   d. There is no real difference; all hacking is considered unethical.

9. What is the purpose of antivirus software?
   a. to increase the speed of the computer's processor
   b. to protect against known threats and analyze system behavior to detect new threats
   c. to manage the organization's email server
   d. to offer technical support for software developers

10. What is the primary aim of a distributed denial-of-service (DDoS) attack?
   a. modifying unauthorized data
   b. disrupting the availability of a target's network resources
   c. gaining unauthorized access to secure data
   d. causing physical damage to the network infrastructure

11. What is a key process of an effective information security risk management (ISRM) strategy?
   a. periodic security training
   b. continuous monitoring
   c. single-layer security
   d. annual risk assessments

12. COBIT5 is an example of what type of ISRM resource?
   a. a compliance framework
   b. a risk management plan
   c. a network security protocol
   d. an incident response system

13. What organization is well known for developing standards and frameworks like COBIT to support compliance with ISRM practices?
   a. IEEE
   b. ISO
   c. ISACA
   d. NIST

14. What is the first step in developing a comprehensive risk management plan?
   a. identifying risks

b. implementing controls
c. assessing risks
d. establishing the context

15. Why is continuous monitoring in an ISRM strategy important?
a. It allows for one-time setup of complete security controls.
b. It helps eliminate all cyber risks.
c. It ensures security measures are effective over time against evolving threats.
d. It provides a static security environment.

16. Why is it important to integrate continuous monitoring with other security processes?
a. to ensure compliance with COBIT5 only
b. to guarantee zero risk posture
c. to reduce the need for security training
d. to maintain a comprehensive approach to organizational security

17. Who is responsible for implementing security measures to protect an organization's data and ensuring that these measures are aligned with regulatory requirements?
a. security consultant
b. compliance analyst
c. security software developer
d. threat intelligence analyst

18. What role does continuous learning play in the field of cybersecurity?
a. to stay updated with the latest cybersecurity trends and technologies
b. to maintain a static skill set over time
c. to focus solely on traditional cybersecurity methods
d. to decrease the need for professional certifications

19. In the context of cybersecurity, what does the term "digital trust" primarily refer to?
a. the encryption standards used in digital communications
b. the confidence stakeholders place in an organization's ability to secure data and systems
c. the digital certificates used for website authentication
d. the trustworthiness of digital signatures

20. What is a significant cybersecurity challenge posed by the rise of cloud computing?
a. simplified IT infrastructure
b. decreased data storage needs
c. unique risks such as data breaches, unauthorized access, and compromised integrity of shared resources
d. reduced need for network security

21. In which type of organization would a Certified Information Security Manager (CISM) certification be especially beneficial for career advancement?
a. tech start-ups
b. government agencies
c. financial institutions
d. nonprofit organizations

22. Which role is essential for creating strategies to protect against large-scale cyber threats and managing an organization's overall cybersecurity posture?
a. network security administrator
b. chief information security officer (CISO)
c. IT support technician

d. cybersecurity legal advisor

Check Your Understanding Questions

1. Explain the role of encryption in network security and why it is considered a key principle.
2. What are some common network vulnerabilities, and how can they pose a threat to the integrity and availability of a network?
3. What is a common security vulnerability found in many web applications, and what countermeasure can be implemented to mitigate this risk?
4. Why is it important to consider ethical issues when performing penetration tests?
5. Explain why it is important for an ISRM strategy to have clearly defined roles and responsibilities within an organization.
6. What are the essential elements to include in a comprehensive risk management plan?
7. What are the primary responsibilities of a CISO, and how do they differ from those of an information security analyst?
8. Identify and describe the types of organizations where information security careers are most viable and explain why these organizations are optimal for such roles.

Application Questions

1. Reflect on the ethical implications of the distinction between information security and information privacy. How do these two concepts impact personal freedom and responsibilities in a digital age?
2. Consider a scenario where ethical considerations might conflict with legal requirements in the context of securing information and networks. How would you navigate such a situation?
3. Watch this video on developing an ISRM strategy (https://openstax.org/r/109ISRMstrategy) from ISACA Live. Search for an ISRM case study and look for some of the elements discussed. What elements discussed in the video are missing from the ISRM case study you found?
4. Should managers depend solely on IT people to solve all security challenges? (*Hint*: Consider the types of decisions made by general managers versus IT managers.)
5. Consider the sectors that are currently most at risk for cyberattacks. How do you think the demand for information security roles within these sectors will evolve in the next five years?
6. How would you describe the job of a cybersecurity engineer/manager to someone who does not work in the tech field?

6 Enterprise Security, Data Privacy, and Risk Management

Figure 6.1 Continuous threats to data privacy and security encourage organizations to develop policies and protocols that evolve with technology. (credit: modification of work "Data Security Breach" by blogtrepreneur.com/tech/Flickr (http://blogtrepreneur.com/tech/Flickr), CC BY 2.0)

Chapter Outline

Introduction

Many of us turn a key in our door lock or press a button on our car's key fob as a routine habit. It's quite easy to lock up our living space or keep our vehicle secure. But how do we keep information secure? How can we protect data the way we protect more tangible items around us? In today's digital environment, most of our interactions, transactions, and online engagement create a footprint of data that can be cataloged, tracked, and used for a wide array of purposes. While data can help enterprises tailor personalized experiences for customers or make insightful business decisions, it also brings to the forefront important considerations about data protection, data integrity, and responsible computing. The issues of security, privacy, and risk in information systems are of increasing importance in our modern digital landscape.

6.1 Key Concepts in Data Privacy and Data Security

Learning Objectives

By the end of this section, you will be able to:

- Define data privacy and data security and their importance to the enterprise
- Identify the risks and consequences of not protecting personal data and sensitive information
- Describe how enterprise security and risk policies impact data privacy
- Identify various data privacy regulations and standards mandated to protect privacy information

The state in which data are kept from unauthorized access through the proper handling, processing, storage, and usage of data regarding consent, notice, and regulatory obligations is called **data privacy**. Its primary focus consists of individuals' rights to reasonable protection of their personal information from unauthorized access, disclosure, or abuse. Additionally, **data security** is an element of data privacy and involves the implementation of measures to ensure data are kept safe from corruption and unauthorized access while preserving confidentiality, integrity, and availability (CIA).[1]

Data privacy and security are critical to any enterprise for several reasons, including trust and reputation, prevention of financial loss, mitigation of financial risks, and controlled operational risks. Trust in this sense refers to the confidence that consumers have in relation to an organization, while reputation is the collective perception or evaluation of an organization.

Several data protection and management tools have been developed to further bolster efforts to keep data safe. They involve the assessment and mitigation of privacy risks, the implementation of privacy engineering, and the design of products and services that inherently respect and protect the privacy of individuals. Any breach can significantly damage an enterprise's reputation and consumer trust.[2] To this end, several regulations, such as the European General Data Protection Regulation and the California Consumer Privacy Act, require businesses to protect personal data under threat of penalties and other legal actions.

The Importance of Enterprise Digital Data Privacy and Data Security

Data privacy and security play a critical role in our ever-expanding digital world. As businesses, governments, and other large enterprises transition to digital platforms, the amount of data created has exponentially increased. Historically, small companies and large enterprises have sought to contain their trade secrets, customer information, and intellectual property rights through training and other mitigating measures. In a nondigital landscape, access to sensitive information was often controlled through **physical security**, which is the protection of buildings, hardware, and assets. This included measures such as locked cabinets, secure rooms, and need-to-know restrictions, where only those with explicit permission could access certain data. Personnel were trained to handle information carefully, and physical controls were in place to ensure that unauthorized individuals couldn't gain access. However, as technology has advanced, more data are now being stored electronically, transmitted via the internet, and accessed from the cloud. Thus data are now much more susceptible to breaches, accidental disclosures,and exploitation by bad actors. A **bad actor** is a person or entity who hacks or cracks into a computer or system with malicious intent. Data privacy involves ensuring the responsible use of personal information throughout the data life cycle, and it underpins the fundamental principles of ethical business practices. For example, a customer signs up for an online service, and their data are collected, stored, and used for account setup and personalized recommendations. After the service is canceled, the data are archived for compliance purposes and eventually deleted following retention policies.

It is no secret that unauthorized access to confidential data, often leading to the exposure of sensitive information, called a **data breach**, occurs often. However, what is staggering is the sheer number of user accounts that have been compromised as a result. For example, in April of 2024, billions of records from a background check service known as National Public Data (NPD) were exposed, affecting hundreds of millions of people. The exposed records contained sensitive items such as Social Security numbers, birth dates, and mailing addresses.[3]

In 2024, a data breach involving AT&T compromised approximately 100 million customer records, exposing sensitive personal information, including names, addresses, and Social Security numbers. This incident highlighted vulnerabilities in data storage and the growing challenges of securing customer information

1 Kim B. Schaffer, Peter Mell, Hungh Trinh, and Isabel Van Wyk, "Recommendations for Federal Vulnerability Disclosure Guidelines," *NIST Special Publication 800-216*, National Institute of Standards and Technology, May 24, 2023, https://doi.org/10.6028/NIST.SP.800-216

2 Hsiangting Shatina Chen and Tun-Min Jai, "Trust Fall: Data Breach Perceptions from Loyalty and Non-Loyalty Customers," *The Service Industries Journal*, 41, no. 13–14 (2021): 947–963

3 Daniel Hooven, "2.9 Billion Reasons To Be Concerned—The Latest on the National Public Data Breach," Schnieder Downs, August 21, 2024, https://schneiderdowns.com/our-thoughts-on/npd-breach/

against increasingly sophisticated cyberattacks.

Another major breach in 2024 affected Change Healthcare, a service provider to UnitedHealth. A ransomware attack disrupted health-care operations nationwide, affecting claims processing and payments for weeks. It was revealed that sensitive medical data, such as diagnoses, test results, and treatments for a substantial proportion of Americans, had been stolen. The financial and operational fallout from this attack underscored the critical importance of cybersecurity in health care.

Information generation has not grown in a steady, linear fashion; rather, it has increased exponentially as companies have leveraged digital assets to maintain growth amid competition. For example, in the late 1970s, the internet was in its early stages of development. The World Wide Web became publicly available in 1991, and at that point, the internet was primarily text-based with limited multimedia content. As shown in Figure 6.2, the internet is remarkably different today from its original iteration.

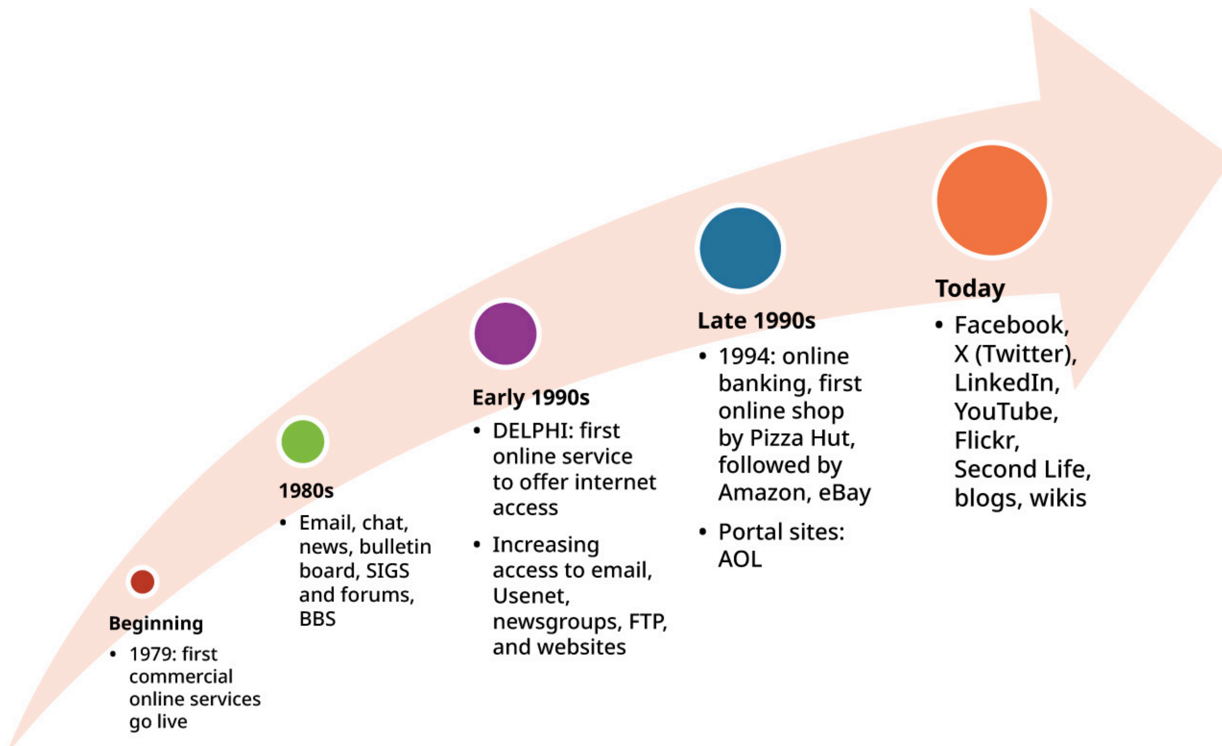


Figure 6.2 The World Wide Web has seen many improvements and expansions since its first development in 1979. (credit: modification of work "History of online service" by "Viviensay"/Wikimedia Commons, CC0 1.0)

The volume of data has increased exponentially due to the digital evolution, with global internet traffic growing from 100 GB per day in 1992 to 150.7 TB per second by 2022,[4] driven by vast amounts of content generated and shared across various platforms. These figures highlight the explosion of data generation and consumption over the past few decades, an explosion that's been driven by technological advancements and the digitization of various aspects of life. The challenge today lies not only in managing the volume of this data, but also in harnessing it effectively and ethically. In other words, it is a complex challenge that underscores the importance of data privacy and security.

4 World Bank, *World Development Report 2021: Data for Better Lives* (World Bank, 2022), https://doi.org/10.1596/978-1-4648-1600-0

FUTURE TECHNOLOGY

The Future of Data Provenance

As entities continue to collect data from various devices, websites, and social media platforms, an important issue has arisen concerning the proper handling, integrity, and usage of that data. One concept known as data provenance has emerged as a potential solution to reduce the threats of data mishandling, contamination, and leakage. Data provenance refers to the documentation of a dataset's life cycle, which is essential for ensuring data quality and adherence to laws, regulations, and policies governing the industry or operation, or compliance. There are three pillars that comprise data provenance:

- Source provenance: tracking the origins of data
- Transformation provenance: documenting the changes and processes the data undergo
- Usage provenance: details on how data are accessed and used

Data provenance ensures trust and transparency, aids in meeting compliance with legal requirements, and facilitates data reuse and reproducibility.

Data privacy and security are no longer mere IT issues. Rather, they form an essential aspect of an enterprise's strategic planning. Today, businesses are expected to be stewards of the data they hold, protecting information from breaches and ensuring its appropriate use. As a result, enterprises are investing significantly in data security measures and privacy protocols to safeguard customer data (and thereby maintain trust) and to comply with increasingly stringent regulations. Security breaches can result in massive financial and reputational damage. Thus, the need for robust data privacy measures is critical.

Consider the cases of Solar Winds and MGM Resorts. Solar Winds is a company that develops software to manage and control computer networks. It was targeted in 2020 in an attack that affected thousands of organizations globally and highlighted how vulnerable even the most sophisticated, well-protected networks are.[5,6] In 2023, MGM Resorts in Las Vegas, Nevada, was one victim of a ransomware attack that caused significant outages of systems such as door locks, key card readers, and other hotel amenities. The damage from the attack cost MGM over $100 million in lost revenue and was executed through BlackCat operators who used social engineering techniques to gain access to critical systems.[7] These attacks underscore that data privacy is integral to maintaining consumer trust and the smooth operation of critical infrastructure, and in extreme cases could be a national security concern.

Finally, it is essential to acknowledge the international dimensions of data privacy. In an interconnected world where enterprises often operate across borders, understanding the nuances in privacy regulations and practices in different regions is key because the location of the source of the data takes precedence over the customer's citizenship location. Whether it's the more consumer-centric privacy model of the EU's General Data Protection Regulation (GDPR), the sector-specific approach in the United States, or the diverse and evolving landscape of data privacy regulations in Asia and Australia, businesses need to be equipped to navigate these varying landscapes while upholding their commitment to data privacy and security.

5 Cybersecurity and Infrastructure Security Agency, "Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise," U.S. Department of Homeland Security, May 14, 2021, https://www.cisa.gov/news-events/news/remediating-networks-affected-solarwinds-and-active-directorym365-compromise

6 Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," U.S. Department of Homeland Security, April 15, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

7 Arielle Waldman, "MGM Faces $100M Loss from Ransomware Attack," TechTarget, October 6, 2023, https://www.techtarget.com/searchsecurity/news/366554695/MGM-faces-100M-loss-from-ransomware-attack

Risks and Consequences of Unprotected Personal Data and Sensitive Information

Unprotected personal data and sensitive information pose a variety of risks, with far-reaching consequences that extend beyond the digital realm. Cyber threats such as data breaches and **identity theft**—which is the act of stealing someone's information and assuming their identity—represent some of the most immediate risks of unprotected personal data. Sometimes bad actors may wait for months or years before exploiting the breached data to prevent suspicion that the data have been breached.

In 2024, IBM's annual *Cost of a Data Breach* report revealed that the global average cost of a data breach has reached $4.88 million, marking a 10 percent increase from the previous year. This underscores the growing financial impact of data breaches on organizations worldwide.[8] Beyond the financial loss, a data breach can also result in a severe loss of customer trust, tarnishing the organization's reputation. This may take years to rebuild and could lead to a long-term decrease in the company's market value.

One of the most striking examples of this is the Equifax breach in 2017, which exposed the personal information, including Social Security numbers, of nearly 147 million people. In its aftermath, the company faced hundreds of millions of dollars in legal fees and reparations, and the value of its stock fell by more than 30 percent.[9] As of 2024, Equifax has had to pay over $425 million to users affected by the breach and has invested in over $1.6 billion to improve security and technology.[10]

Cyber Espionage

The use of online methods to obtain secret or confidential information without the permission of the holder of the information, typically for strategic, military, or political advantage, is considered **cyber espionage**. The risk of cyber espionage continues to escalate, with unprotected personal data often being the target. A notable example from 2022 is the Uber data breach, where an attacker compromised the company's internal systems. This incident exposed a vast amount of sensitive data and disrupted Uber's operations. The breach not only raised concerns about the protection of user and employee data, but also highlighted vulnerabilities in corporate cybersecurity practices. Additionally, the persistent threat of ransomware attacks remains a major concern. These attacks, which involve hijacking an organization's data for ransom, have seen a significant rise in sophistication and frequency, further emphasizing the need for robust data security measures.

Reputational Harm

Unprotected personal data and sensitive information pose a significant risk to both businesses and individuals. Data can be exploited for fraudulent activities, identity theft, and other malicious acts. But the repercussions of inadequate data protection extend beyond immediate financial harm and can significantly damage an organization's reputation and erode customer trust. Trust is a critical element of customer loyalty and a significant factor in a business's success. When customers provide businesses with their personal data, they are entrusting those businesses to keep their information safe. A data breach can lead to a breach of that trust, which can be challenging to restore.

According to IBM's report, the largest contributor to the costs associated with data was "lost business," which includes customer attrition, reputation damage, increased customer acquisition costs, and lost revenue opportunities.[11] One high-profile example of this is the 2013 Target data breach, which resulted in the theft of the credit and debit card information of 40 million customers. This breach cost Target approximately $291 million and caused significant damage to its reputation. Their sales decreased dramatically in the last quarter of 2013, and fewer households reported shopping at Target.[12]

---

8 IBM, *Cost of a Data Breach Report: 2024* (IBM, 2024), https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

9 "Equifax to Pay $700m over Breach That Exposed Data of 150m People," *The Guardian*, July 22, 2019, https://www.theguardian.com/us-news/2019/jul/22/equifax-data-breach-security-ftc-settlement

10 John Egan, "Five Years after the Equifax Data Breach, How Safe Is Your Data?," Bankrate, September 12, 2022, https://www.bankrate.com/credit-cards/news/how-safe-is-your-data/

The rise of privacy-conscious consumers, those who are aware of and concerned about how their personal data are collected and distributed, means that businesses need to be even more diligent in their data protection efforts. A 2020 Cisco report found that 84 percent of consumers care about data privacy, and 80 percent are willing to act to protect it—meaning they would switch away from companies that have poor data practices or policies.[13] Organizations must continue to invest significantly in data security measures and privacy protocols to safeguard their customer's data, maintain trust, and comply with increasingly stringent regulations.

How Enterprise Security and Risk Policies Impact Data Privacy

Enterprise security and risk policies are fundamental in shaping an organization's approach to data privacy. To ensure the effectiveness of these policies, organizations often turn to established frameworks such as those recommended by the Information Systems Audit and Control Association (ISACA), where white papers and research articles offer valuable insights into best practices. The *MIS Quarterly Executive (MISQE)*, *Journal of Management Information Systems (JMIS)*, *Communications of the ACM (CACM)*, *Journal of the Association for Information Systems (JAIS)*, and *Communications of the AIS (CAIS)* serve as reputable sources of the latest advancements in the science of privacy. While Privacy by Design and privacy engineering are closely related, they focus on different, albeit complementary, goals. Privacy by Design aims to integrate privacy considerations into the design and operation of IT systems, business practices, and networked infrastructure right from the outset.

Privacy by Design and Privacy Engineering

To make these principles actionable, standards such as the ISO/IEC 27701 for privacy information management, and frameworks such as Privacy by Design (PbD) by Ann Cavoukian[14] are invaluable. Cavoukian characterized this **Privacy by Design** approach as proactive more so than reactive; it anticipates privacy invasion events before they occur. These tools allow businesses to convert abstract, principles-based legal mandates into implementable technical privacy controls compatible with existing security measures. The Privacy by Design model employs seven principles, such as being proactive and embedding privacy, into the design (Figure 6.3). By adhering to such standards, organizations can mitigate risks and foster trust, which is particularly vital in an age where data breaches and cyberattacks are increasingly sophisticated and damaging.

11 IBM, *Cost of a Data Breach Report: 2024* (IBM, 2024), https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

12 Kelli Young, "Cyber Case Study: Target Data Breach," Coverlink Insurance, September 12, 2021, https://coverlink.com/cyber-liability-insurance/target-data-breach/

13 Cisco, *Protecting Data Privacy to Maintain Digital Trust* (Cisco, 2020), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf

14 Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, 2008, https:/privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf

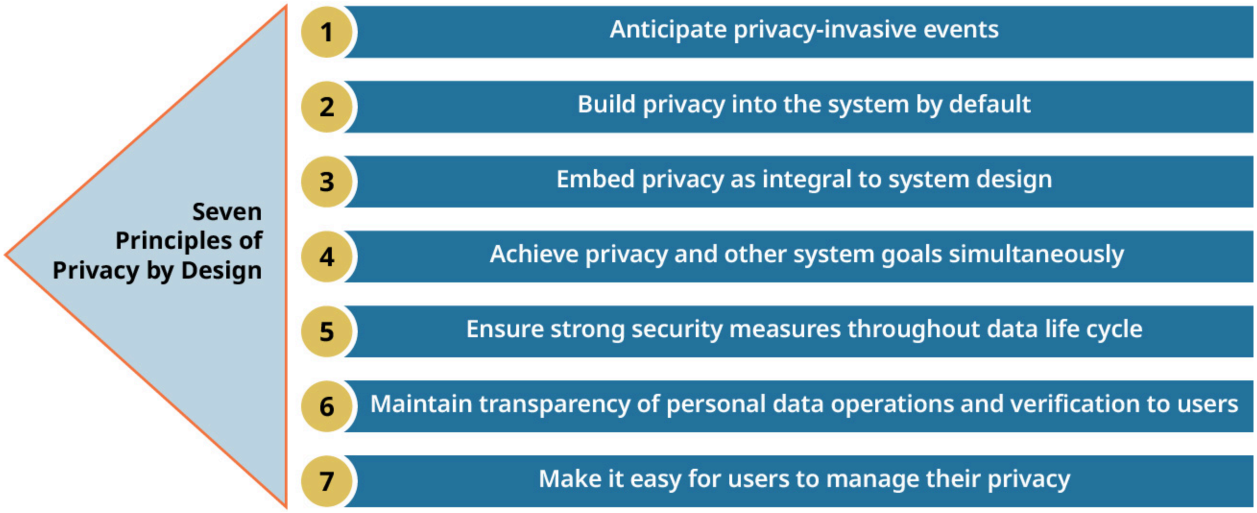


Figure 6.3 There are seven foundational principles of Privacy by Design. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Considering all these threats, several national and international organizations, corporations, and governments have taken measures to promote data protection and integrity. Through features such as app tracking transparency and clear privacy labels on the App Store, Apple provides users with greater visibility and control over how their data are used, although the overall architecture of their system remains relatively closed compared with more open platforms.

Data scientists suggest that data are providing an endless stream of new digital capital. However, organizations that fail to take data privacy and security seriously may lose their competitive edge as well as customer trust, and/or face regulatory action. Tackling the massive scale and complexity of data management requires the implementation of robust, risk-based frameworks.

An emerging field in this context is **privacy engineering**, which is fundamentally about incorporating privacy principles directly into the design and development of IT systems, networks, and business practices. By making privacy an integral part of the design and development process rather than an afterthought, enterprises can effectively mitigate risks and better protect user data. Some examples of privacy engineering include:

- Google's Differential Privacy: This practice allows Google to leverage the ability to learn from aggregate data while ensuring that returned search results and map addresses do not permit anyone to learn about a particular individual. Google has used this with Google Maps to help show the busy times at restaurants and other locations without divulging the location history data of users.
- Apple's Privacy Labels: Apple has developed Privacy Labels for its App Store. These labels provide simple, straightforward summaries of an app's privacy practices, and they are written in plain language, letting consumers know what data an app collects and whether the data are linked to them or used to track them.
- Microsoft's Data Loss Prevention (DLP): Microsoft developed a data loss prevention solution to prevent sensitive information from leaking out of the organization. This solution identifies sensitive information across several platforms, such as Exchange Online, SharePoint, OneDrive for Business, and Microsoft Teams. This measure ensures that data are not inadvertently shared with the wrong groups. While DLP does well with implementing controls that prevent data loss, it does not focus on physical security.

On the other hand, privacy engineering refers to the technical and operational aspects of implementing privacy principles in systems and services. Its goal is to operationalize the concepts of Privacy by Design through specific methodologies, tools, and technologies. Privacy engineering focuses on developing practical solutions and practices that protect individuals' privacy and meet regulatory requirements. This includes creating data protection features, ensuring secure data processing, and developing privacy-preserving technologies. While Privacy by Design sets the framework and objectives for privacy, privacy engineering focuses on actual implementation of those objectives in the real world. Like Privacy by Design, privacy engineering focuses more on the technical aspects of implementing data protection controls. One example of a social media company that uses this idea is Snapchat, which limits the amount of time a message can be viewed once it is sent.

CAREERS IN IS

Data Privacy and Security Career Options

With its ever-evolving challenges and emerging practices, the area of data privacy and security offers many exciting opportunities. Those seeking to work in this field may consider these roles, for example:

- Privacy analyst/privacy consultant: A specialist who assesses and advises organizations on complying with data protection laws and regulations. They analyze privacy policies, conduct privacy impact assessments, and recommend strategies to protect personal data.
- Chief privacy officer (CPO): A high-level executive responsible for an organization's data privacy policies and procedures. The CPO ensures compliance with privacy laws, oversees data protection strategies, and manages privacy risks.
- Cybersecurity analyst: A professional who focuses on protecting an organization's computer systems and networks. They monitor breaches, investigate security incidents, and implement security measures to safeguard sensitive data.
- Information security manager: A role responsible for overseeing and managing an organization's information security program. They develop and implement policies and procedures to protect data from unauthorized access, disclosure, alteration, and destruction.
- Compliance officer: A role that involves ensuring an organization meets external regulatory requirements and internal policies, especially concerning data protection and privacy laws.
- Data protection lawyer: A legal professional specializing in data protection and privacy law. They advise clients on compliance with data protection regulations, represent in case of data breaches, and help draft privacy policies.

Third-Party Risks

A key aspect of security and risk policies is the management of third-party risks, including **third-party access**, which is access to data from an external entity. In an interconnected digital ecosystem, organizations often share data with partners, vendors, and other third parties. This is particularly significant given the rise of cloud computing, which is the delivery of computing services over the internet, and Software as a Service (SaaS), which is a software distribution model in which applications are hosted by a third-party provider and made available to customers over the internet, typically on a subscription basis. For instance, Amazon Web Services, Google Cloud, and Microsoft Azure handle vast amounts of data from countless businesses. These enterprises must ensure that their security policies cover these relationships and that third parties meet stringent security standards.

The measures that enterprises can adopt include regular audits and inspections, solid contractual agreements regarding data handling, and clear communication about responsibilities in the event of a security breach. Furthermore, an enterprise's data might be shared with a third party not only for storage purposes, but also for processing. Many businesses employ third-party data analytics firms to make the most of their collected information.

FUTURE TECHNOLOGY

Two Privacy Developments on the Horizon

The future of technology in information systems paints a promising picture for data privacy and protection. Here's a brief look at two key developments:

- Federated learning: An emerging concept in machine learning, federated learning allows a model to be trained across multiple decentralized devices or servers holding local data samples, without exchanging the data samples themselves. This helps to maintain privacy as raw data never leave their original device.[15]
- Homomorphic encryption: A form of encryption allowing computations to be carried out on encrypted data, homomorphic encryption produces an encrypted result that, when decrypted, matches the result of operations performed on the plain data. This means sensitive data can be processed securely in encrypted form, without ever needing to be decrypted, thereby maintaining data privacy.[16]

These technologies demonstrate how the future of information systems may uphold robust data protection while still leveraging the benefits of data-driven insights. As these technologies mature, they will play an increasingly significant role in securing information systems and ensuring data privacy.

For stakeholders such as investors and partners, solid security policies imply the organization's proactive stance toward risk management, which can increase their confidence in the organization's resilience against potential data breaches. The best policies will be those that keep evolving with the changing technology landscape and regulatory environment, continuously fostering a culture of privacy and accountability in the organization. In **accountability**, people and entities must take responsibility for the decisions they make and be able to explain them.

Data Privacy Regulations and Standards

Data privacy regulations and standards have become increasingly important in today's data-driven world. With vast quantities of personal data being collected and processed daily, these regulations ensure the safeguarding of personal information and provide a standardized approach for businesses to manage data privacy. Across the globe, nations are developing regulations to address this ever-evolving need. For example, the Personal Data Protection Act (PDPA) in Singapore strives to protect personal data across the economy by serving as a complement to sector-specific legislative and regulatory frameworks.[17] Meanwhile, in Brazil, the Lei Geral de Proteção de Dados (LGPD) came into effect in August 2020, aligning the country more closely with the global trend toward stricter data privacy regulations.[18] The **General Data Protection Regulation (GDPR)** is a comprehensive data protection law in the European Union that sets guidelines for the collection and processing of personal information of individuals within the EU.[19] The GDPR represents a major shift in data privacy regulations. It has introduced several significant changes, including stricter requirements for **consent**, which is the explicit permission given by an individual for the collection, processing, and use of their personal information. Additionally, the GDPR expanded data subject rights (such as the right to be forgotten, the right to data portability, and the right to object to processing), and steeper penalties for noncompliance, up to 4 percent of an organization's global annual turnover or 20 million euros, whichever is higher.[20]

15 Brendan McMahan and Daniel Ramage, "Federated Learning: Collaborative Machine Learning without Centralized Training Data," Google Research, April 6, 2017, https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/
16 Kirsty Paine, "Homomorphic Encryption: How It Works," Splunk, February 5, 2024, https://www.splunk.com/en_us/blog/learn/homomorphic-encryption.html
17 "PDPA Overview," Personal Data Protection Commission Singapore, accessed December 22, 2024, https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act
18 Lei Geral, *Lei Geral de Proteção de Dados (LGPD),* Obtenido de Lei Geral de Proteção de Dados (LGPD), 2020, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

In a similar manner, the **California Consumer Privacy Act (CCPA)**, a law that increases privacy rights and consumer protection for residents of California, has set a benchmark for data privacy in the United States[21] (Table 6.1). While it only applies to businesses that meet certain criteria (such as having gross annual revenues over $25 million), the CCPA is influencing data practices beyond California. It is likely to inspire similar legislation in other states, or potentially at the federal level.[22] Under the CCPA, businesses must disclose what data they collect, sell, or share, and consumers can opt out of the sale of their data, request deletion of their data, or access the data that businesses have collected about them.

	CCPR	GDPR
Implementation date	July 1, 2020	May 25, 2018
People affected	For-profit companies that collect personal data on California residents	EU citizens, businesses, data subjects, and controllers
Application	Businesses, third parties, California residents	Organizations offering goods and services in the EU
Data scope inclusions	Any personal data sold for monetary or other value	Any type of personal data
Fines for noncompliance	$7,500 per violation and $100–$750 per consumer incident related to breaches	Up to 20 million euros for major violations; up to 10 million euros for minor violations

Table 6.1 Comparison of the CCPR and GDPR The U.S.'s California Consumer Privacy Act (CCPA) and the E.U.'s General Data Protection Regulation (GDPR) are two regional regulations that provide foundational frameworks for cybersecurity.

However, it's not just regulatory compliance that organizations need to consider. Industry standards also play a crucial role in shaping how businesses protect personal data. For instance, the International Organization for Standardization (ISO) has introduced ISO/IEC 27701, an extension to ISO/IEC 27001, the international standard for information security management systems. ISO/IEC 27701 provides guidance on how to manage privacy information, essentially translating privacy principles from regulations like the GDPR into actionable controls. This involves not only technical measures, but also administrative ones, such as defining roles and responsibilities, maintaining records of processing activities, and ensuring proper data breach response procedures.[23] By adopting ISO/IEC 27701, organizations can demonstrate their commitment to privacy, reassure customers and stakeholders, and potentially gain a competitive advantage.

Businesses will also need to consider other relevant regulations in their respective jurisdictions. For instance, in Canada, businesses must comply with the Personal Information Protection and Electronic Documents Act (PIPEDA), which establishes basic rules for the use, collection, and disclosure of personal information by private sector organizations during commercial activities. Similarly, in Australia, the Privacy Act 1988 mandates how personal information is to be handled.

Moving forward, as data privacy issues continue to rise in prominence, we can expect further evolution in both

19 European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Official Journal of the European Union, L119 (2016): 1–88, https://eur-lex.europa.eu
20 "GDPR Fines/Penalties," Intersoft Consulting, accessed December 22, 2024, https://gdpr-info.eu/issues/fines-penalties/
21 California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 - 1798.199), Enacted as AB-375, California Legislative Information, 2018, https://leginfo.legislature.ca.gov
22 "AB-375 Privacy: Personal Information: Businesses," California Legislative Information, June 29, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
23 International Organization for Standardization, *ISO/IEC 27701:2019* (ISO, 2019).

legislation and industry standards. Companies will need to stay vigilant and adaptive, not just to avoid penalties, but also to earn and maintain their customers' trust and loyalty. This is particularly true in an era where data privacy is increasingly seen as a differentiator and a competitive advantage. Trust in how businesses handle personal data can significantly impact their brand reputation, customer relationships, and, ultimately, their bottom line.

The landscape of data privacy is becoming increasingly complex, and staying abreast of these regulations and standards is crucial for businesses.

6.2 Vulnerabilities and Threats in Web Applications and IoT Technology

Learning Objectives

By the end of this section, you will be able to:

- Identify common vulnerabilities and threats in web applications and IoT technology
- Determine the countermeasures and techniques used to combat threats of security and privacy of web applications and IoT technology
- Discuss the social responsibility of enterprises and IT professionals developing this technology
- Determine guidelines or regulations that must be implemented to protect web applications and IoT technology in the future

Every connected device you own is collecting data—about your preferences, routines, and even your health. This data, if compromised, can lead to significant privacy breaches. As we become increasingly reliant on IoT technology, it is essential to recognize the risks that come with it. The concern is not just about securing your smartphone or computer. It is about securing a network of devices that know more about you than you might realize.

The solution rests in understanding the inherent vulnerabilities of web applications and IoT technology and recognizing the potential threats that exploit these weaknesses. In our age of extensive data collection and usage, commitment to transparency, accountability, and privacy protection becomes a cornerstone of responsible innovation. Examining these issues requires exploring privacy and security risks associated with the web and IoT technology, potential countermeasures, ethical considerations, and prospective regulatory frameworks.

Common Online Vulnerabilities and Threats

In the span of a few decades, digital technology has transformed the world. The arrival of the mobile revolution introduced an era of smartphones, bringing the internet from the confines of home and office spaces into the palms of our hands. The digital revolution continued with the equipping of even the simplest items with internet connectivity, forming the core of the modern digital era.

The **Internet of Things (IoT)**, a term coined by Kevin Ashton in 1999, is the network that connects everyday physical objects to the internet, enabling them to collect and share data with other devices or systems. The IoT now encapsulates a vast array of everyday items from refrigerators and thermostats to door locks and light bulbs, converting them into smart, connected devices (Figure 6.4). The sheer scale of IoT's growth is nothing short of astounding. To put it in perspective, in 2003, the number of devices connected to the internet was estimated at around 500 million.[24] By 2018, that number had increased to 10 billion.[25] And the number of IoT devices in use globally is expected to reach 40 billion by 2030.[26]

24 Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group (IBSG), April, 2011, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
25 Insider Intelligence, "How IoT & Smart Home Automation Is Entering Our Homes in 2020," *Business Insider*, January 6, 2020. https://www.businessinsider.com/iot-smart-home-automation
26 "Satyajit Sinha, Connected IoT Devices Forecast 2024–2030," from *State of IoT 2024: Number of Connected IoT Devices Growing 13% to 18.8 Billion Globally*, IoT Analytics, September 3, 2024, https://iot-analytics.com/number-connected-iot-devices/

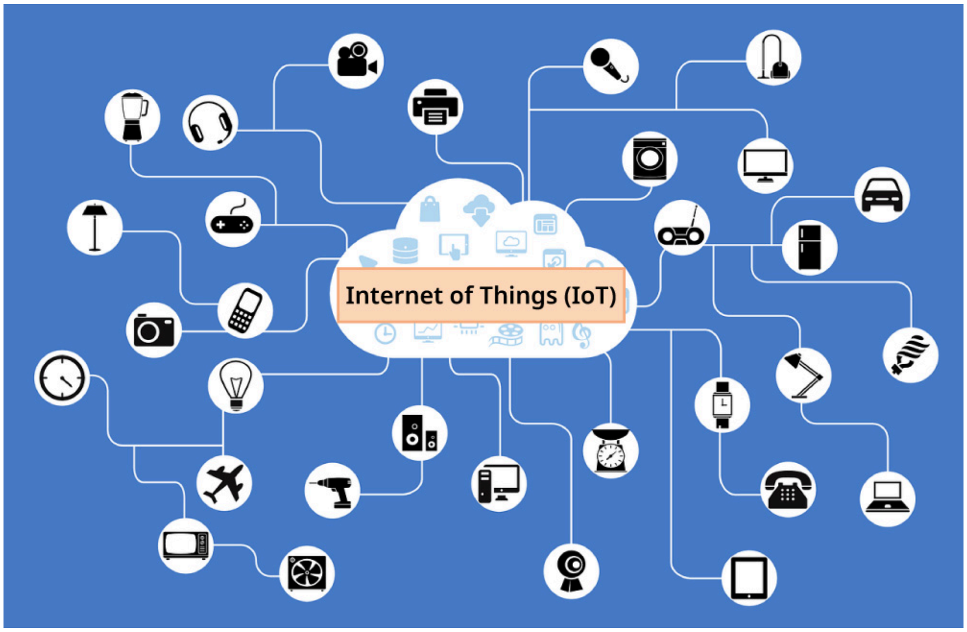


Figure 6.4 An interconnected group of IoT devices can communicate with the cloud and each other independently. (credit: modification of work "Internet et ses applications" by "jeferrb"/Wikimedia Commons, CC0 1.0)

This rapid expansion of the IoT has significant implications, both positive and negative. On one hand, it creates new opportunities for innovation, efficiency, and convenience as smart homes equipped with IoT devices can automate a variety of tasks, from adjusting the thermostat to managing home security systems. However, the proliferation of IoT devices also introduces substantial security vulnerabilities both at home and at work. The introduction of these devices into the workplace further complicates security for IT managers because vulnerabilities in IoT devices often allow attackers to eavesdrop, conduct brute-force attacks, and elevate their privileges on a network.

Keeping pace with the rapid advancement in IoT technologies and adequately addressing the myriad security risks they present is a significant challenge for regulatory bodies. The sheer number of IoT devices and the rapid growth of that number, plus their widespread distribution, further complicate regulation. These devices, often manufactured in one region, sold in another, and potentially operated in a third, create a transnational landscape that can blur jurisdictional lines and make enforcement of regulations challenging. Additionally, the proprietary nature of many IoT devices poses its own set of problems. In many instances, device manufacturers prioritize time to market and functionality over security, leading to devices with hard-to-patch vulnerabilities. Some manufacturers might use proprietary protocols, which are tools specific to the organization and closed off to the public, making it difficult for regulatory bodies to assess and ensure their security.

The high-profile Mirai botnet attack of 2016 serves as an important real-world example of these challenges. This was a distributed denial-of-service (DDoS) attack that exploited many inherent weaknesses in IoT security: default passwords, unsecured network services, and the lack of regular software updates in many devices. The attack targeted and overwhelmed the servers of Dyn, a major DNS provider, with a tremendous amount of traffic. This disruption impacted several high-profile platforms and services, including Twitter, Netflix, Reddit, and CNN, rendering them inaccessible to millions of users for several hours. This incident showcased how easily IoT devices can be exploited for malicious purposes and the far-reaching consequences of such security lapses.

Similarly, IoT technology is transforming industry practices. Industry 4.0, which represents the fourth industrial revolution noted by the integration of digital technology in manufacturing and digital practices, allows for real-time monitoring, predictive maintenance, and increased operational efficiency. However, these devices also present a potential entry point for cyberattacks, risking not only data breaches, but also physical damage and potential safety hazards.

Given the expansive growth and diverse applications of IoT technologies, one thing is clear, while IoT devices bring a multitude of benefits, they also carry significant risks. As we continue to incorporate these technologies into various facets of life, it is important to understand and mitigate these vulnerabilities.

Web Applications: Banking and E-commerce

Among the most prevalent and potentially damaging threats in the digital realm are those targeting web applications, particularly in sectors like banking and e-commerce. A study by the security firm Positive Technologies found that 100 percent of web applications contain at least one security vulnerability, with 48 percent of these vulnerabilities considered high risk.[27] Online banking systems are prime targets for cybercriminals due to the sensitive nature of the information they handle.

Techniques like phishing—wherein users are tricked into providing their login credentials to fake websites—and SQL injection—where hackers exploit a vulnerability in a web application's database query software—can result in unauthorized account access and monetary loss. Similarly, e-commerce platforms face threats such as credit card fraud, DDoS attacks, and cross-site scripting (XSS), which is a type of vulnerability that allows an attacker to inject malicious scripts into websites trusted by end users, leading to potential theft of sensitive data such as login credentials or credit card information.

IoT Technology: Smart Homes and Self-Driving Cars

IoT technology has transformed sectors such as home automation and transportation, and as more devices become connected to the internet, the potential for vulnerabilities increases. Smart homes, with internet-connected security systems, thermostats, and appliances, are particularly susceptible to threats such as device hijacking, where attackers gain control over IoT devices. Similarly, self-driving cars, which rely on complex systems and sensors, face significant cybersecurity risks, as many of their systems were not originally designed with security in mind. In 2024, a high-profile incident occurred when researchers demonstrated the ability to remotely hack into the infotainment system of a Tesla, gaining access to critical vehicle functions.

ETHICS IN IS

German Steel Mill Attacks

ThyssenKrupp, a major German steel producer, was targeted by a sophisticated cyberattack in early 2024. The attack disrupted the operations of its automotive division, forcing parts of the facility offline to contain the threat. Although full details have not been disclosed, the attack demonstrated the ongoing vulnerability of industrial control systems (ICS) in the manufacturing sector. The incident involved cybercriminals gaining unauthorized access to critical systems. Another attack on a German steel mill ten years prior used spear-phishing tactics to infiltrate the office network before accessing the plant's production networks. Attackers manipulated control systems, causing significant physical damage, including a blast furnace that could not be properly shut down. This event marked a pivotal moment in understanding the real-world dangers of cyberattacks on industrial systems.

Both incidents highlight the increased risks associated with the convergence of operational technology (OT) and information technology (IT) networks. This integration, a hallmark of the Industrial Internet of Things (IIoT), has expanded the attack surface, making industrial facilities more susceptible to cyber threats. The ThyssenKrupp attack serves as a stark reminder that even with advancements in cybersecurity, industrial control systems remain vulnerable to sophisticated cyber threats, with the potential for substantial physical damage.

27 "Threats and Vulnerabilities in Web Applications 2020–2021," Positive Technologies, June 13, 2022, https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020-2021/

Frameworks to Identify Vulnerabilities and Protect IoT/IT Ecosystems

The IoT ecosystem, marked by its complexity and breadth of use cases, presents its own set of regulatory challenges. Unlike more traditional, monolithic systems, IoT is characterized by a multitude of interconnected devices, platforms, and services, spanning across various sectors and geographical boundaries. One example would be a "smart" refrigerator communicating with a smartphone to replenish grocery items by adding them to the grocery shopping list for home delivery and communicating this information to the grocery store identified by the homeowner.

This variety of devices and tasks not only introduces numerous potential vulnerabilities but also makes it difficult to apply a one-size-fits-all regulatory framework. One of the primary regulatory challenges in IoT is its vast and rapidly evolving nature. IoT devices range from simple sensors to complex industrial systems, each with different security requirements and implications.

As such, it is necessary to examine the existing structure of rules and guidelines, often legislated, within which an industry or business must operate, or the **regulatory framework**.

Organizations such as the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE) have developed standards, such as ISO/IEC 27001 and IEEE 2413, to address these vulnerabilities through risk management frameworks and architectural guidelines. The ISO/IEC 27001 provides the framework for an information security management system (ISMS), which is a systematic approach consisting of processes and procedures designed to control an organization's information security risks. An ISMS allows organizations to manage security in a comprehensive and structured manner, ensuring that all potential vulnerabilities are addressed and that systems are resilient to potential attacks. The IEEE has been heavily involved in developing standards for IoT. One such standard is the **IEEE 2413**, an architectural framework for IoT that aims to promote cross-domain interaction, aid system interoperability and functional compatibility, and foster a common understanding among IoT systems.

International standards offer guidelines that help ensure the robustness, security, and interoperability of web and IoT technologies. They also provide a basis for creating regulations and laws that can govern these technologies in different regions worldwide. Cities adopting smart technologies often rely on these international standards to ensure the reliable and secure operation of their systems. For instance, another standard from the ISO, ISO/IEC 30141, provides a reference architecture for IoT, assisting the developers and operators of smart city solutions in creating systems that can securely communicate and interact.

However, since current regulations such as GDPR and CCPA are region-specific, there is a need for more comprehensive global regulations. Countries such as the United Kingdom, Brazil, and India are developing specific IoT security laws, reflecting a trend toward targeted regulatory measures. For example, Brazil's Lei Geral de Proteção de Dados (LGPD) and India's Personal Data Protection Bill reflect global concerns regarding data privacy. Countries such as the United Kingdom have initiated specific guidelines for IoT device security, focusing on secure passwords and regular updates. New regulatory trends such as these require different stakeholders to adapt. Businesses must understand and comply with various international regulations, making it necessary to invest in legal expertise. Consumers benefit from these protections, and as a result, they develop confidence in digital services.

Regulators face challenges, however, in balancing consumer protection with enabling technological innovation. Future challenges may arise from the integration of IoT with 5G networks, quantum computing, and decentralized technologies such as blockchain. These advancements will necessitate a reevaluation of existing regulations and potentially lead to new regulatory frameworks. Strategies may include international collaboration to standardize regulations across jurisdictions, fostering innovation while maintaining security. For example, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) is a system privacy framework designed to facilitate the secure flow of personal information across APEC borders while maintaining strong privacy protections.

Industry-led self-regulation extends beyond established examples such as Payment Card Industry Data Security Standard (PCI DSS), which is a set of standards designed to ensure companies secure credit information. For example, the Center for Internet Security (CIS), a nonprofit organization that works to safeguard private and public organizations against cyber threats, provides guidelines that organizations can voluntarily follow. The Industrial Internet Consortium (IIC)—which is an organization that accelerates the growth of the industrial internet by promoting best practices, reference architectures, and frameworks—has released a security framework to guide industries in building secure IoT systems.

In addition, the Internet of Things Security Foundation (IoTSF) provides a comprehensive set of guidelines and best practices for securing IoT devices. The continually evolving landscape of IoT and web regulations, combined with the increasing role of self-regulation by the industry, emphasizes the importance of understanding various global regulations and guidelines. These include well-known examples such as GDPR and CCPA, plus emerging trends such as LGPD, IIC, and IoTSF. Adapting to these changes requires ongoing vigilance, collaboration, and commitment to balancing innovation with ethical principles and consumer protection.

CAREERS IN IS

Careers in Security

Due to the rapid proliferation of technology, there's a growing need for professionals who can navigate the security challenges these technologies present, such as the following:

- Web security analyst: identifies and mitigates vulnerabilities in web applications such as SQL injection and XSS
- IoT security specialist: secures connected devices by recognizing and addressing vulnerabilities unique to IoT environments
- Ethical hacker: tests vulnerabilities in web and IoT technologies, exploiting weaknesses and recommending countermeasures
- Corporate social responsibility (CSR) officer: ensures that web and IoT technology development aligns with ethical and social responsibility initiatives
- Policy analyst: studies and influences regulations related to web and IoT security, drafting guidelines for improved protection
- Privacy engineer: designs and implements privacy solutions for IoT devices and web applications in compliance with regulations
- Compliance auditor: ensures web and IoT technologies adhere to industry standards and regulations, safeguarding business integrity

Countermeasures to Combat Online Security Threats

With an ever-increasing reliance on interconnected digital technologies, security risks continue to escalate. Cybersecurity incidents have the potential to cause not only digital disruption, but also substantial real-world impacts. There is an array of strategies designed to manage the risks associated with these technologies, from preventive measures such as secure coding and data encryption to reactive solutions such as incident response plans. These countermeasures help professionals better navigate the challenges of technological advancement and safeguard digital environments.

Implementing Secure Coding Practices

Securing web applications begins with secure coding practices. Because code is one of the key elements of a digital system, poor coding practices can inadvertently introduce vulnerabilities that bad actors can exploit to compromise these systems and cause data breaches or service disruptions. One notable example of a data breach that took advantage of coding errors is that of First American Financial Corporation, a leading provider of title insurance and settlement services to the real estate and mortgage industries. In 2019, hundreds of millions of documents related to mortgage deals going back to 2003 were leaked due to a coding issue that permitted attackers to access unauthorized information by manipulating the URL of the website. [28]

These practices encompass various activities such as validating input, ensuring proper error handling, and maintaining the principle of least privilege. Following guidelines such as the OWASP Secure Coding Practices can help developers avoid common pitfalls that lead to vulnerabilities in the code. Secure coding practices include the following:

- Systems should always check inputs received from users or from other systems for their data type, length, format, and range, a process called **input validation**. Any input that does not meet these requirements should be rejected.
- Every module or process should follow the **least privilege principle**, in which users are granted the minimum levels of access, or permissions, needed to perform their job functions, reducing the risk of unauthorized access to sensitive information. If a function only needs to read from a file, it should not have write access to the file. This reduces the potential damage that can be done if the function is compromised. If a malicious actor gains control of a process, they are restricted by the permissions of that process. For example, if a database query only needs to retrieve data, it should not have permission to alter or delete the data.
- Implement strategies and coding practices to effectively identify, report, and manage errors that occur during the operation of a software application or system. Potential errors need to be systematically managed and addressed to prevent system failures and security breaches, known as **error handling**.

Strengthening Authentication and Authorization

The importance of robust authentication and authorization mechanisms in web applications cannot be overstated. In such applications, user credentials typically serve as the keys to unlocking a massive amount of sensitive information and services. Hence, their protection helps maintain the integrity and confidentiality of these resources as well as user trust.

Multifactor authentication (MFA), biometric identification, and risk-based authentication are among the strategies that can significantly bolster the authentication and authorization process. MFA, which requires the user to provide two or more verification factors, adds an extra layer of security, making it harder for attackers to gain access even if they compromise one factor. Biometric identification, such as fingerprints or facial recognition, provides a unique verification method that is difficult to replicate, thereby enhancing security. Risk-based authentication adjusts the authentication process based on the risk level associated with the user's behavior or access conditions. Such an approach allows for a balance between security and usability, offering a more robust protection mechanism when needed.

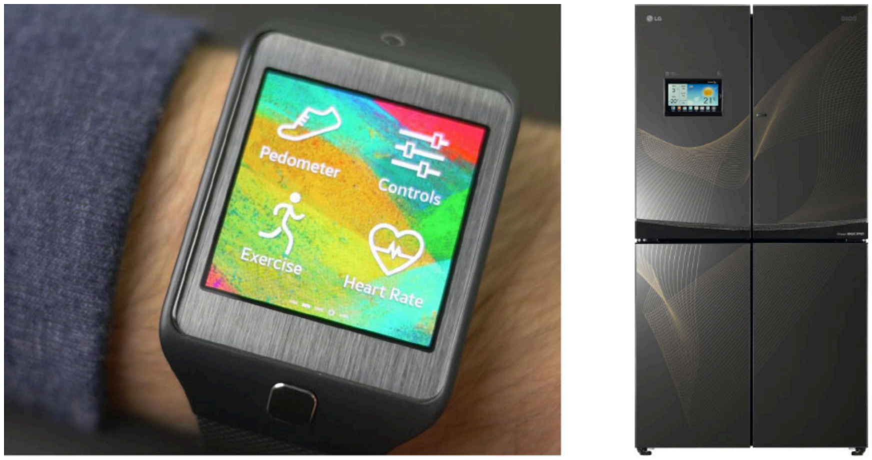
Designing for Security and Hardware Measures

As you learned in Chapter 5 Information Systems Security Risk Management, technologies such as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) play a vital role. These systems identify possible threats and deploy measures to mitigate them.

A predominant concern in IoT is the integral need for security starting from the very roots. For example commonplace items such as home appliances, vehicles, and personal devices have become embedded with

28 United States of America before the Securities and Exchange Commission, *Securities Exchange Act of 1934: Administrative Proceeding, File No. 3-20367*, in the matter of First American Financial Corporation, Respondant, Release No. 92176, June 14, 2021.

IoT technology, thereby extending IT concerns beyond their traditional confines (Figure 6.5).



(a) (b)

Figure 6.5 IoT technology is seen in everyday items, such as (a) smartwatch technology and (b) smart refrigerators. (credit a: modification of work "Health 11" by The IET/Flickr, Public Domain; credit b: modification of work "LG Smart DIOS V9100" by LG Electronics/Wikimedia Commons, CC BY 2.0)

Maintaining security of IoT devices involves regular firmware updates. These updates play a dual role: first, they bring new features and rectify bugs, and second, they patch security vulnerabilities, which is key to preserving the security of the device throughout its life cycle. Further critical to IoT security is **secure device onboarding**, which involves adding devices to the network in a secure manner that prevents unauthorized access and protects the integrity of the network.

Social Responsibility of Enterprises and Information Technology Professionals

Technology has permeated virtually every aspect of modern life, largely propelled by the proliferation of IoT and web applications. This pervasive integration of IoT has brought to the forefront a range of ethical considerations that were once limited to more clearly defined technological areas. It now encompasses not only privacy and data security, but wider societal issues such as accessibility, inclusivity, environmental sustainability, and professional ethics. This evolution underscores the critical need for a comprehensive understanding and proactive management of ethical concerns in all areas of technology.

Ethical Considerations in Information Technology

Data handling and management, professional responsibilities, and promoting digital inclusivity are critical ethical considerations in the field of IT. Key aspects of these principles include:

- Data collection, storage, processing, and sharing:
  - Collecting: Enterprises must be transparent about the nature and purpose of data collection, ensuring users are fully informed.
  - Storing and processing: Robust security measures are necessary to prevent unauthorized access and potential misuse, safeguarding sensitive information.
  - Sharing: Data sharing practices should prioritize user privacy and adhere to relevant regulations, ensuring that information is treated with respect.
- Professional responsibilities of IT professionals:
  - Protecting user data and ensuring privacy
  - Promoting accessibility and reducing the digital divide
  - Upholding fairness and inclusivity within the digital realm
- Adherence to professional codes of ethics:

- Complying with codes of ethics from organizations such as the Association of Computing Machinery (ACM) and IEEE that guide IT professionals in ethical decision-making
- Operating under key principles such as respecting privacy, avoiding harm, performing with honesty and trustworthiness, and contributing to society and human well-being

- Digital inclusivity and accessibility:
  - Ensuring equal access to technology, regardless of socioeconomic background, geographical location, or physical abilities
  - Designing technology with accessibility in mind benefits diverse user needs, improving both reach and user experience

LINK TO LEARNING

View the entire ACM Code of Ethics (https://openstax.org/r/109ACMCodeEthic) here.

LINK TO LEARNING

Point: Some scholars assert that technology companies have an inherent moral duty to prioritize human well-being in their operations, citing ethical theories such as utilitarianism (https://openstax.org/r/109Utilitarian) and corporate social responsibility.

Counterpoint: Others argue that the primary responsibility of these enterprises is to their shareholders (https://openstax.org/r/109Shareholders) and that ethical considerations, while important, should not overshadow business objectives.

Role of Enterprises in Promoting Digital Inclusivity and Accessibility

Ensuring everyone has equal access to technological advances is an important social issue. Digital inclusivity, which entails making IT solutions available and accessible to all, has a profound impact on narrowing the digital divide. The **digital divide** refers to the gap between individuals, communities, or countries that have access to modern information and communication technologies and those that do not. This divide can manifest in various forms, such as differences in internet access, digital literacy, and the availability of affordable devices and services. Tech enterprises have the responsibility to foster an inclusive digital environment. By developing affordable and accessible technologies, they can ensure that the benefits of digital innovation reach all corners of society and that users can effectively utilize these solutions.

This necessitates designing technology with diverse user needs in mind. From building websites that are accessible to individuals with visual or hearing impairments, to creating software that is easy to navigate for individuals with cognitive or motor skill challenges, the commitment to accessibility is a cornerstone of ethical IT development. Designing with accessibility in mind not only widens the user base, but also enhances the overall user experience.

ETHICS IN IS

Ethical Decision-Making in IT

To illustrate the importance of ethical decision-making, consider the case of a social media platform deciding to implement a new data-sharing policy. Adherence to ethical principles would mean that the platform informs its users about the policy changes in a clear and transparent manner, allows users to opt out if they desire, and implements robust measures to protect shared data. In contrast, an unethical approach would be to implement the policy covertly without informing users or obtaining their consent. A real-world example of not following ethical principles was demonstrated by Facebook in 2014.

Facebook faced significant controversy when it was revealed that the company had covertly conducted a psychological experiment on nearly 700,000 unsuspecting users. The experiment, carried out in 2012, involved manipulating users' news feeds to either reduce the number of positive posts or reduce the number of negative posts they saw. The objective was to determine whether the changes could sway users' emotions and influence their subsequent posts. The results suggested that emotional states could be transmitted across the social network, leading to a ripple effect.

However, the study's execution sparked significant backlash. Critics argued that Facebook had manipulated users' emotions without their explicit consent, raising serious ethical concerns regarding user consent and the boundaries of corporate research. The incident served as a stark reminder of the need for clearer guidelines and transparency when conducting research on platforms with such extensive user bases. This conversation about ethics and transparency was further highlighted in U.S. Senate Committee on the Judiciary's congressional hearings during 2024 when lawmakers scrutinized the impact of social media on teens' mental health and the ethical responsibilities of tech companies.

Transparency and Accountability

Transparency has become a significant ethical issue in IT. In the context of organizations and governance, **transparency** refers to openness, communication, and accountability, where actions and decisions are clear and understandable to stakeholders. Users have the right to know how their data are collected, stored, used, and shared. Enterprises need to be transparent in their data practices, providing clear and understandable privacy policies and consent mechanisms. Transparent practices not only meet regulatory requirements, but also foster trust between users and enterprises, which is crucial for long-term user engagement.

The roles of tech enterprises and IT professionals in being accountable for the social and ethical implications of technology have never been more critical. Both entities are key stakeholders in shaping the norms and values of the digital realm. Enterprises must imbue their business strategies with ethical considerations, from protecting user data to ensuring digital inclusivity. Likewise, IT professionals, the frontline workers of the digital revolution, must adhere to professional ethical codes, conscientiously delivering solutions that honor user rights and societal values. It is through their collective efforts that technology can truly serve its purpose as a tool for advancing societal well-being.

Social Responsibility in the Information Technology Sector

The obligation of companies to act in ways that benefit society and the environment beyond what is legally required is considered **social responsibility**. In the IT sector, social responsibility is expected to evolve and deepen as emerging technologies such as artificial intelligence, IoT, and blockchain raise new ethical questions that will require innovative and thoughtful responses. As these technologies become increasingly integrated into everyday life, the ethical dimensions of IT will extend beyond individual user rights to encompass broader societal impacts, including sustainability. The future will call for an even stronger commitment from enterprises and IT professionals to uphold ethical standards, promote transparency, ensure digital inclusivity, and champion sustainability.

6.3 Data Security and Privacy from a Global Perspective

Learning Objectives

By the end of this section, you will be able to:

- Identify global frameworks in data security and privacy
- Identify global regulations and requirements for data security and privacy
- Apply a framework to a case study

In an era driven by digitization and the Internet of Things (IoT), vast amounts of data are generated, collected, processed, and transmitted daily. From personal user preferences in online shopping to critical health data, information flows through global networks with an ease previously unimaginable. Data have indeed become one of the most valuable commodities in the modern era, both for businesses and for bad actors, making the frameworks that guide its safekeeping vitally important to maintaining the integrity of our digital future.

Reflecting the diverse concerns of different regions and industries, several frameworks have emerged that now serve as a universal staple in data management practices of multiple private, public, and governmental organizations. These frameworks, such as the COBIT 2019, the Enterprise Privacy Risk Management Framework, and the ISO/IEC 27701, provide structured practices that enable enterprises to comply with regulatory demands and establish and maintain a culture of data integrity and privacy-centric operations. These international standards are critical as they shield enterprises from potential breaches and legal repercussions in the respective country.

However, the world of data security and privacy is in a perpetual state of evolution. The introduction of landmark regulations such as the European Union's GDPR or California's CCPA is testament to the shifting sands of data governance, with each new regulation aiming to balance business innovation with individual rights. In navigating this dynamic terrain, organizations must not only be aware of these frameworks and regulations, but also thoroughly understand their nuances and the underlying principles they champion.

Global Frameworks in Data Security and Privacy

Due to the explosive growth and constant evolution of technologies frameworks have been established through the collaboration of international standards organizations, governmental bodies, and industry groups to establish guidelines that resonate on a worldwide scale. Some of the most well-known are the globally recognized COBIT 2019 Framework, the Enterprise Privacy Risk Management Framework, ISO/IEC 27701, and the NIST Privacy Framework.

COBIT 2019 Framework

Developed by the Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technologies (COBIT) stands out as a comprehensive framework designed for the governance and management of enterprise IT. While its primary focus is IT governance, its principles and guidelines offer a holistic approach to robust data protection. The framework, previously known as COBIT5 and then overhauled in 2019, emphasizes the importance of stakeholder needs, risk management, and a value-based, holistic approach that aligns IT goals with business objectives. Organizations employing this framework may use it to:

- establish a systematic approach to managing personal data
- ensure that privacy risks are identified and mitigated
- demonstrate compliance with privacy regulations globally
- foster trust among stakeholders, especially data subjects, by showcasing a commitment to privacy

An example of COBIT adoption is the European Network of Transmission System Operators for Electricity (ENTSO-E).

Tasked with representing forty-two electricity transmission operators across thirty-five European countries, ENTSO-E embarked on a journey in 2014 to integrate COBIT 5 into its IT processes.[29] This strategic move was aimed at refining the organization's intricate IT infrastructure to support massive electricity flows, establish a decade-long network development blueprint, and ensure a transparent, standardized energy transaction framework across Europe. By embracing COBIT 5, ENTSO-E was able to fortify its IT governance, ensuring data integrity, process efficiency, and a commitment to excellence in line with its ambitious mission.

As the framework evolved, they have continued to align their practices with the updated COBIT 2019 to address emerging IT governance challenges.

ISO/IEC 27701

An extension to the ISO/IEC 27001 and ISO/IEC 27002 standards, the **ISO/IEC 27701** provides guidelines for establishing, implementing, and maintaining a **privacy information management system (PIMS)**, which is a framework or set of policies and procedures used by an organization to manage personal data and ensure compliance with privacy laws and regulations.

ISO/IEC 27701 is particularly vital given the volume of international and regional data protection laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States.

The key highlights of ISO/IEC 27701 include three levels (Table 6.2):

- Frameworks and Standards (Top Level): These are the overarching guidelines that organizations follow. For instance, ISO/IEC 27001 is the standard for managing information security, while ISO/IEC 27701 focuses on privacy.
- Systems (Middle Level): The frameworks lead to the creation of specific systems such as ISMS and PIMS, which are implemented within organizations to protect information and ensure compliance.
- Sector-Specific Applications (Bottom Level): The standards and systems are applied differently across sectors, acknowledging that each has specific requirements and challenges.

Standards, Systems, and Sectors	Application
Top Level: Frameworks and Standards	
ISO/IEC 27001	Foundation for information security management system (ISMS)
ISO/IEC 27002	Provides best practices and controls to support the ISMS established by ISO/IEC 27001
ISO/IEC 27701	An extension of ISO/IEC 27001 and 27002, focused on privacy information management system (PIMS)
Middle Level: Systems Examples	
Information security management system (ISMS)	Created based on ISO/IEC 27001, this system manages and protects an organization's information

Table 6.2 ISO/IEC 27701 Hierarchy The hierarchy of the ISO/IEC 27701 provides guidance through overarching standards, specific systems, and the application of those standards and systems.

29 European Network of Transmission System Operators for Electricity, "Net-Zero Industry Act," ENTSO-E, July 2023, https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Publications/Position%20papers%20and%20reports/2023/ENTSO-E%20NZIA%20Position%20Paper_%20June2023.pdf

Standards, Systems, and Sectors	Application
Privacy information management system (PIMS)	Built upon ISO/IEC 27701, this system integrates privacy controls into the ISMS, focusing on personal data protection
Bottom Level: Sector-Specific Applications	
Health-care sector	Adoption of ISO/IEC 27701 to ensure patient data privacy across borders
Financial services sector	Utilization of ISO/IEC 27701 to manage global client data securely
Tech sector	Integration of ISO/IEC 27701 into cloud platforms to safeguard user data

Table 6.2 ISO/IEC 27701 Hierarchy The hierarchy of the ISO/IEC 27701 provides guidance through overarching standards, specific systems, and the application of those standards and systems.

NIST Privacy Framework

In January 2020, the National Institute of Standards and Technology (NIST) released its Privacy Framework to address the challenges of increasing data privacy risks. This framework complements the NIST Cybersecurity Framework, specifically focusing on managing privacy risks by promoting the idea of Privacy by Design, which is a concept and approach in system engineering and data handling practices that integrates privacy and data protection measures from the very beginning of the design process, rather than as an afterthought.

The NIST Risk Management Framework allows enterprises to translate high-level, principles-based legal requirements into tangible technical privacy controls. Figure 6.6 outlines the Risk Management Framework steps, serving as a blueprint for organizations to tailor their own cybersecurity strategies. Notably, it incorporates guidance from a suite of NIST standards. For instance, NIST SP 800-39 offers a broad overview for managing information security risk organization-wide, while IR 8062 provides a nuanced approach to privacy engineering and risk management. SP 800-30, on the other hand, specializes in risk assessments, helping organizations identify, evaluate, and prioritize risks.

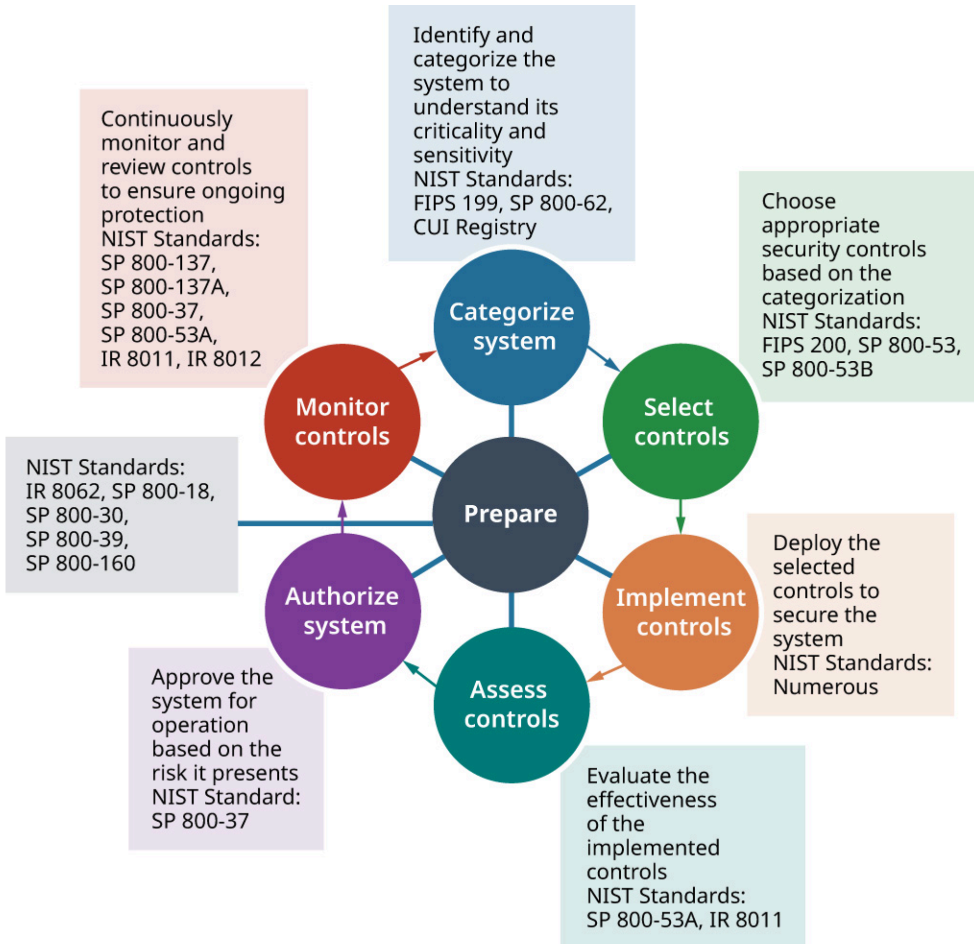


Figure 6.6 The Risk Management Framework steps incorporate key NIST standards such as SP 800-39 for organizational risk, IR 8062 for privacy engineering, and SP 800-30 for risk assessments. (modification of work “Risk Management” by NIST/National Institute of Standards and Technology, Public Domain)

As we advance further into the era of data-driven decision-making and digital innovation, these frameworks and regulations play a dual role. First, they provide a framework to guard against potential risks, and second, they lay the foundation for businesses to innovate responsibly, ensuring that user trust isn’t compromised.

National Regulations outside the United States and the European Union

The growing number of regulations and standards creates complexity for multinational companies, requiring significant resources and expertise to comply with different, sometimes conflicting, regulations. These challenges include addressing security risks due to inadequate security controls in IoT devices, differing standards across devices, and issues of data sovereignty in cloud-based platforms and access controls. International alignment and cooperation in data privacy regulations is crucial, as it simplifies compliance for global businesses and facilitates international trade and data flows.

In a globalized world where technology transcends borders, the protection of user information, data security, and privacy controls is a shared concern among nations, although each country has its own regulatory laws. Just as the United States has put in place various agencies and standards to oversee data protection, other nations across Asia, South America, and Africa have crafted comparable frameworks to safeguard user information.

China: Personal Information Protection Law

China’s Personal Information Protection Law (PIPL), introduced in 2021, marks the country’s first major data privacy law. This law is crucial for ensuring that personal information collected within China remains within its borders—a concept known as data localization. PIPL sets very strict rules for sharing data with other countries, meaning that companies must meet specific requirements before transferring data out of China. These requirements include getting certifications or contracts that align with Chinese standards.

Japan: Act on the Protection of Personal Information

Japan's Act on the Protection of Personal Information (APPI) has been a key part of the country's data privacy laws since it was first enacted in 2003. Recognizing the growing importance of global data protection, Japan made significant changes to the APPI in 2017 to update it in line with international standards, such as the European Union's GDPR. The APPI focuses heavily on individual rights, ensuring that people have control over their personal data. This includes the right to access their data, correct any inaccuracies, and decide how their data are used. Businesses are required to clearly explain why they are collecting personal data and must obtain explicit consent from individuals.

South Africa: Protection of Personal Information Act

South Africa's Protection of Personal Information Act (POPIA), which became fully effective in 2021, is designed to protect the privacy of personal data within the country. POPIA applies to any organization that processes personal information in South Africa, whether the data are processed automatically (like on a computer) or manually. The law requires that organizations are transparent about why they are collecting personal data and that they get consent from individuals when necessary. POPIA also emphasizes the importance of lawful processing, meaning that data can only be used for legitimate purposes. Furthermore, organizations must appoint an information officer to oversee compliance with POPIA, ensuring that the organization follows the regulations.

Industry-Specific Regulations and Standards

In the rapidly evolving landscape of information security, two frameworks stand out for their comprehensive approach and widespread adoption: the Payment Card Industry Data Security Standard (PCI DSS) and ISO/IEC 27001 (Table 6.3). PCI DSS, a global security framework, sets the standard for safeguarding cardholder information, thereby playing a crucial role in mitigating credit card fraud.

Framework	PCI DSS	ISO/IEC 27001
Purpose	• Increases controls around cardholder information • Aims to reduce credit card fraud	• Helps organizations manage information security practices • Aligns information security with business needs
Governance	• Maintained by the Payment Card Industry Security Standards Council • Applicable to all entities handling credit card data	• An international standard; part of the ISO/IEC 27000 family • Establishes, implements, maintains, and improves an ISMS

Table 6.3 Industry-Specific Regulations and Standards The PCI DSS and ISO/IEC 27001 purposes, governance, data protection, security measures, and impact on organizations are laid out in their frameworks.

Framework	PCI DSS	ISO/IEC 27001
Data protection and risk management	• Requires strong encryption for storing and transmitting cardholder data • Establishes secure network requirements through firewalls and other measures	• Provides guidance on managing and mitigating information security risks • Emphasizes regular risk assessment and mitigation strategies
Security measures/ maintenance and improvement	• Mandates regular security testing and assessments • Limits cardholder data access to necessary personnel only	• Includes ongoing maintenance and continuous improvement of the ISMS • Ensures regular reviews and updates to security practices
Compliance and impact/adoption and impact	• Mandatory for organizations handling branded credit cards • Enhances customer trust by indicating high-security standards	• Widely adopted across various industries as a security benchmark • Improves information security management and competitive advantage

Table 6.3 Industry-Specific Regulations and Standards The PCI DSS and ISO/IEC 27001 purposes, governance, data protection, security measures, and impact on organizations are laid out in their frameworks.

The enforcement of these security standards and regulations typically involves a combination of government oversight, industry self-regulation, and third-party audits. Government agencies in various countries develop and enforce regulations, often imposing penalties for noncompliance, which can include fines, legal action, or operational restrictions. Compliance with these standards is often verified through third-party audits conducted by accredited certification bodies, which assess whether organizations meet the required security and privacy benchmarks.

Effective collaboration between nations, industries, and regulatory bodies is essential in shaping a coherent, effective approach to data protection in the globalized digital age.

Case Study: Attaining ISO/IEC 27001 Certification

Information security remains at the forefront of organizational priorities, particularly as data breaches and cyber threats become increasingly sophisticated. The ISO/IEC 27001 certification differentiates organizations that have excelled in establishing robust information security processes and procedures to safeguard crucial data. Additionally, organizations that meet this standard are better equipped to prevent data breaches and protect essential data. This case study delves into the experience of a Texas-based **data center**, a facility designed to host computer systems and related components, as it tackled the challenges of securing this vital certification during the global COVID-19 pandemic.

Background: The ISO/IEC 27001 Standard

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly developed ISO/IEC 27001. This globally recognized standard specifies the requirements for establishing, implementing, maintaining, and continuously improving an information security management system (ISMS). An organization that achieves this certification demonstrates its commitment to information security and data privacy, meeting international standards of excellence.

ISO/IEC 27001 certification is achieved through a rigorous process facilitated by a **certification body**, which is an organization accredited to assess and certify that companies, systems, processes, or products meet the established standards and requirements. The traditional method to obtain this certification involves undergoing an **audit**, a systematic examination and evaluation of an organization's records, compliance with regulatory standards, and the integrity of financial reporting processes.

The Challenge: Certification during a Pandemic

In April 2020, Lone Star Data Hub, a data center located in Austin, Texas, embarked on a journey to achieve ISO/IEC 27001 certification. For Lone Star Data Hub, known for managing critical data infrastructure for regional clients in sectors such as finance and health care, this certification was more than just a seal of approval. It was a strategic business move aimed at setting their services apart in a competitive market. Obtaining ISO/IEC 27001 certification would underscore the center's dedication to stringent information security standards and enhance its appeal to a broad client base, including Fortune 500 companies. This certification was seen as a crucial step in demonstrating their commitment to protecting sensitive data and maintaining the highest level of security. However, the onset of the COVID-19 pandemic introduced a myriad of challenges, specifically, nationwide lockdowns, social distancing mandates, and the transition to remote work.

To meet the challenges of this certification process, the data center sought a certification body with a solid reputation, even in remote settings. Guided by a recommendation from another auditor and the influence of stakeholders with a comprehensive background in information security, they selected the National Sanitation Foundation; International Strategic Registrations chapter (NSF-ISR).

The ensuing audit was thoroughly planned, with NSF-ISR providing a comprehensive agenda designed to allow the data center to operate seamlessly, ensuring minimal disruption to its ongoing operations. The audit process involved a detailed examination of the data center's information security practices, including assessments of security controls, risk management processes, and compliance with ISO/IEC 27001 standards. This balanced approach provided the data center with invaluable insights, highlighting areas of strength and those needing improvement.

LINK TO LEARNING

Understanding the physical and digital infrastructures that help a data center achieve ISO/IEC 27001 certification can be eye-opening. Explore a real-world ISO/IEC 27001 certified data center (https://openstax.org/r/109ISOIEC27001) through this virtual tour to observe the kind of security protocols and management systems in place. By going through the tour, you'll get an insider's look into the rigorous security measures and operational protocols that these certified facilities maintain. This will help you better understand the significance and implementation challenges of achieving ISO/IEC 27001 certification, and also deepen your understanding of how ISO/IEC 27001 principles are applied in a real-world setting.

Remote Auditing: A New Paradigm

The adoption of **remote auditing**, a practice in which an audit is conducted off-site via video or other technological means, marked a significant shift in the certification process. Traditionally, auditors would be present on-site, directly interacting with systems and personnel. However, the pandemic's constraints necessitated a different approach. NSF-ISR leveraged digital tools and technologies to assess the data center's systems, processes, and policies. During the remote audit, NSF-ISR measured various aspects, including the effectiveness of security controls, the alignment of practices with ISO/IEC 27001 standards, and the overall security posture of the data center. This assessment was conducted through virtual meetings, screen sharing sessions, and digital document reviews, which have become a new norm. While this mode of auditing was novel, it demonstrated that with the right tools and expertise, remote evaluations could be just as effective as their in-person counterparts.

Achieving Certification: Implications and Benefits

The meticulous audit culminated in the data center obtaining its ISO/IEC 27001 certification. This achievement also signaled an auditor's adeptness in remotely verifying an ISMS. For the Texas-based data center, this certification expanded the company's market opportunities, enabling it to respond to business opportunities that mandated stringent information security practices. As more organizations prioritize data security, the demand for ISO/IEC 27001-certified entities is poised to grow.

6.4 Managing Enterprise Risk and Compliance

Learning Objectives

By the end of this section, you will be able to:

- Evaluate policies and discern whether they comply with global frameworks
- Identify gaps and assess risks in an enterprise's policies
- Describe the processes involved in developing, implementing, and monitoring new policies and protocols

As you have learned, the responsibility of safeguarding data security and privacy is not just a regulatory requirement: it is also a cornerstone of business success in our modern data-driven age. For enterprise organizations, this requires **compliance** --the adherence to laws, regulations, and policies governing an industry or operation --to various frameworks. Additionally, it involves a deeper commitment to understanding and continually aligning internal policies and protocols. An entity's **policy** consists of defined guidelines and procedures established by the organization to regulate actions and ensure compliance with legal and ethical standards. Its protocols are the specific, detailed procedures or rules designed to implement policies in practical terms; for example, a data security protocol might specify encryption standards, access controls, and incident response measures to enforce the privacy policy. Aligning policies and protocols with data protection standards is necessary because in today's digital economy businesses increasingly rely on customer data to drive decision-making, innovation, and personalized services. Therefore, earning and maintaining customer trust by responsibly managing their data is essential. This is all achieved by managing enterprise risk and compliance.

Auditing Policy Compliance to a Global Framework

Aligning with global frameworks such as GDPR is an essential step in ensuring that organizations have strong data security and privacy policies. But how exactly does this alignment occur, and what are the specifics involved in ensuring compliance with such a framework? It starts with understanding the GDPR standards and then auditing how well the company's data and data processing activities perform against those standards. An audit is a systematic evaluation of an organization's data privacy and security practices.

Key Principles of GDPR

The GDPR is built around seven key principles: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality (security); and accountability. Understanding these principles is the foundation of any GDPR compliance audit. An audit should begin with an assessment of areas of potential need. Table 6.4 shows an example of how a company might identify potential actions to take in each area.

GDPR Principle	Facebook's Actions
Lawfulness, fairness, and transparency	Reevaluate user consent mechanisms to ensure transparency and fairness Provide clearer information on data usage
Purpose limitation	Scrutinize third-party app policies to ensure data sharing is for specific, lawful purposes
Data minimization	Review whether minimal data transferred policies are fully enforced
Accuracy	Improve data accuracy
Storage limitation	Implement stricter policies on data storage longevity
Integrity and confidentiality (security)	Tighten security measures to prevent unauthorized data access and leaks
Accountability	Enhance accountability by increasing interactions with regulators Communicate compliance with data protection regulations to the public

Table 6.4 Principal Application in Facebook Audit A company can begin an audit by assessing how effectively its policies and protocols are in aligning to the seven key principles of GDPR.

Data Mapping

An audit requires knowing where all types of personal data are stored, processed, and transferred within the organization. Data mapping serves as an essential precursor to effective data governance and compliance. A **data mapping tool**—which is a software application or platform that enables data professionals to automate the process of mapping data fields, attributes, or elements from source systems to target systems or destinations—can be especially useful here. The tools listed in Table 6.5 can automate this process, identifying various data storage points across the organization's infrastructure, including cloud services, databases, and even employee devices.

Tool	Description
OneTrust Data Mapping	Provides a platform specifically designed to help with privacy, security, and data governance, including GDPR compliance; data mapping helps in visualizing data flows and assessing risks
Varonis	Focuses on protecting sensitive data and detecting insider threats; data mapping features also help in GDPR compliance by identifying where personal data reside and who has access
Symantec Data Loss Prevention (DLP)	Offers robust data mapping capabilities that help in discovering, monitoring, and protecting personal data across endpoints, networks, and storage systems

Table 6.5 Data Mapping Tools Data mapping tools can help facilitate parts of an audit.

Tool	Description
McAfee Total Protection for Data Loss Prevention	Offers robust data mapping, policy enforcement, and reporting capabilities; often used in enterprise settings where there's a complex landscape of data to manage
Collibra	Provides data mapping capabilities as part of its broader data cataloging and governance platform; often used by organizations with more mature data governance needs
IBM Guardium	Offers a comprehensive solution for data discovery and classification; particularly robust in dealing with a wide variety of data types and environments, from cloud storage to traditional databases
Informatica	Offers data mapping as part of its broader suite of data governance solutions; particularly effective for complex, large-scale enterprise environments
Microsoft Azure Purview	Provides a unified data governance service that helps organizations achieve GDPR compliance by mapping data across servers and databases, both on-premises and in the cloud
Talend	Offers data mapping as part of its Data Fabric platform, which is useful for enterprises with complex data pipelines
erwin Data Modeling	Helps organizations create a physical, conceptual, and logical map of their data landscape, which can be especially useful for GDPR compliance

Table 6.5 Data Mapping Tools Data mapping tools can help facilitate parts of an audit.

These data mapping tools offer advantages that go beyond mere identification. They can also categorize the identified data according to its sensitivity and the privacy risks it presents, thereby aiding in the prioritization of data protection efforts. For instance, personal identifiers such as Social Security numbers or medical records may be flagged as high-risk data requiring stricter security measures. By providing a more structured, visual representation of how data flows and resides within an organization, these tools allow for more effective planning and implementation of data privacy policies.

Data Processing Activities

The GDPR requires organizations to document how they process data. Therefore, understanding what kind of data are being collected, for what purpose, and how it is being processed and stored is essential. Additionally, the regulation mandates that companies maintain a detailed record of their data processing activities, from data collection to storage and eventual deletion.

This recordkeeping is not just a compliance requirement—it also serves a strategic function by fostering a culture of accountability and transparency. Failing to adhere to this detailed level of documentation can lead to significant legal consequences under GDPR.

In the context of Facebook, which faced public scrutiny for its data handling practices during the Cambridge Analytica scandal, GDPR compliance required the company to reevaluate its third-party app policies meticulously. Specifically, Facebook needed to document the kind of user data that was being accessed by third-party apps and for what purpose. This finding led Facebook to make changes in its API permissions, ensuring that data access by third-party apps would be more restricted and better aligned with GDPR principles. For example, apps would need explicit user consent to collect data and would be limited in what types of data they could collect. Not only does this practice protect the rights of individuals, but it also helps organizations minimize risks and liabilities by ensuring that each data processing activity has a lawful basis and specific purpose.

GDPR Compliance Checklist

Checklists can help an organization ensure that it hasn't missed any critical elements during an audit. Creating a GDPR compliance checklist is an invaluable step in ensuring that all regulatory requirements are met and that no critical elements are overlooked during the audit process. Checklists serve as both a road map for the initial steps of becoming compliant and a measure for ongoing compliance measures. Following that, the checklist usually breaks down GDPR's key principles and provisions into actionable items. For instance, under the principle of "lawfulness, fairness, and transparency," items on the checklist could include establishing lawful bases for data processing, drafting clear and transparent privacy notices, and setting up mechanisms for obtaining and recording consents.

Regular reviews and updates to the checklist are necessary for maintaining compliance, especially in a rapidly evolving digital landscape. Creating and following a detailed GDPR compliance checklist demonstrates a proactive approach to data protection and serves as documentary evidence of an organization's commitment to compliance, which can be particularly useful if regulatory scrutiny ever occurs.

Identifying Gaps and Risks

Aligning with global frameworks is not a one-time task. The dynamic nature of technology, along with changes in regulation and emerging threats, means that organizations must constantly identify and address gaps and risks in their policies. Keeping an enterprise compliant is an ongoing process that demands vigilance, insight, and a proactive approach to risk management. Knowing how to perform a gap analysis, evaluate compliance with global frameworks, and navigate the complex terrain of enterprise risk policies is important for building and maintaining robust and compliant data management systems, and for effectively managing risks in the ever-evolving landscape of enterprise security.

Gap Analysis

The foundation of strong enterprise risk management lies in an organization's ability to perform a **gap analysis**, which is an evaluation of existing policies and protocols, identifying weaknesses and areas that might not align with global data security and privacy standards. As international regulations evolve, organizations must be agile, adjusting their policies to ensure they remain in compliance with frameworks such as GDPR, CCPA, HIPAA, and others. The ability to evaluate and adapt to these global frameworks is more than just a legal necessity; it's a strategic move that can enhance a business's reputation and consequently its ability to gain and maintain consumer trust.

Risk Assessment

The process of identifying potential risks that could negatively impact an organization's assets and business operations and evaluating potential negative outcomes and the likelihood of them occurring is called **risk assessment**. Every data processing activity carries a level of risk, which must be assessed and mitigated. One of the most comprehensive ways to conduct a risk assessment in the context of GDPR is to perform a **data protection impact assessment (DPIA)**. A DPIA is a structured analysis that maps out how personal data are processed and how to minimize the data protection risks to individuals. It often involves evaluating the necessity and proportionality of the data processing activities and requires consultation with relevant stakeholders, including data protection officers (DPOs) and potentially even the data subjects themselves.

For example, an organization would need to conduct a DPIA when changing how user data are shared with third-party apps. This would involve scrutinizing the types of data being shared, the potential risks of this sharing to user privacy, and the measures that could mitigate these risks. They would assess whether the data sharing is necessary for the service to function or whether less intrusive methods are available. Moreover, the DPIA would investigate security measures to ensure the third-party apps have adequate protections in place. After identifying and quantifying risks, the organization then needs to establish measures to mitigate them. These could range from technical solutions such as encryption and access controls to policy measures such as stricter consent requirements or limitations on data sharing. This step also involves determining the residual risks, or the risks remaining after mitigation, to ensure they fall within acceptable levels.

Finally, GDPR requires that risk assessments are not a one-time activity. Risks need to be periodically reviewed and updated, especially when there is a significant change in data processing activities or when there are new insights into potential vulnerabilities and threats. Conducting regular risk assessments and DPIAs demonstrates an organization's commitment to data protection, and it's also a key requirement for GDPR compliance.

Developing, Implementing, and Monitoring Policies and Protocols

An assessment of gaps and risks is an audit that helps identify where an organization's policies and practices align with or deviate from global standards, and it aims to establish the current situation. Once complete, an organization needs to take the findings of the initial audit and use them as a starting point for creating a concrete **action plan**, which is a detailed outline of steps to be taken to achieve a particular goal. This includes creating new policies and protocols that will bring the organization into compliance with GDPR. This goes beyond mere assessment to provide a road map for achieving compliance, which involves identifying what needs to be done and detailing how to do it.

New Policies and Protocols

The first step involves creating new policies that align with GDPR requirements. For example, this might mean overhauling the company's existing third-party data sharing agreements to include more explicit consent mechanisms. When Facebook was faced with this need, it introduced a "Privacy Checkup" tool that serves as a proactive measure to empower users to control their personal information and privacy settings.[30]

This feature guides users through a step-by-step process to review who can see their posts, what kind of personal information is visible to others, and what apps have access to their data. Not only does the Privacy Checkup tool allow users to understand and configure their settings, but it also aligns with Facebook's obligation under GDPR to make data collection transparent and easily understandable. By implementing such a tool, Facebook is also demonstrating accountability—another key GDPR principle—as it shows the company's active efforts to help users manage their privacy. Table 6.6 provides some examples of new or updated policies an organization might introduce after an audit of GDPR compliance.

Policy/Action	Description
Time-limited data retention policies	Develop a policy where user data are deleted or anonymized after a specified period unless renewed consent is obtained, aligning with GDPR's principles of data minimization and storage limitation
Third-party data handling guidelines	Establish stricter policies for third-party developers, including rigorous vetting processes and mandatory compliance checklists, to ensure they handle user data responsibly, in line with GDPR's accountability principle

Table 6.6 Policies and Actions to Align with GDPR Compliance These examples show potential actions a company might plan to take to improve compliance with GDPR.

30 "Guiding You through Your Privacy Choices," Meta Newsroom, January 6, 2020, https://about.fb.com/news/2020/01/privacy-checkup/

Policy/Action	Description
Stricter data security measures	Implement enhanced encryption methods and two-factor authentication as default settings to better safeguard user data, in accordance with GDPR's integrity and confidentiality principle
Automated data processing notifications	Draft new policies that require explicit notification to users when automated decision-making or profiting based on user data occurs, along with an option to opt out, as mandated by GDPR

Table 6.6 Policies and Actions to Align with GDPR Compliance These examples show potential actions a company might plan to take to improve compliance with GDPR.

Legal and Internal Reviews

Any new policies must undergo a legal review to ensure they are compliant with GDPR standards. They should also be vetted by different departments within the organization to check for feasibility, practicality, and effectiveness.

- Legal review for GDPR compliance: Before any policy is finalized, it needs to be reviewed by legal experts specializing in data protection and compliance. For instance, Microsoft undertook a comprehensive legal review when GDPR was introduced to ensure all its products and services were complying.[31]
- Departmental review for feasibility: Once the legal review confirms the draft policies follow GDPR, the next step is to vet them through the various departments that will be impacted. Each department can give insights into how practicable the new policies are. For example, when Salesforce implemented new privacy policies, it engaged multiple departments, including marketing, sales, and customer service, to ensure operational feasibility.[32]
- Executive approval for effectiveness: The final arbiter in the review process is typically the executive leadership of the organization. Its buy-in is critical not just for approval, but also for the effective implementation of the policies. Amazon's leadership, for example, plays an active role in the review and approval of compliance policies, as evidenced by the company's public corporate governance guidelines.[33]

Employee Training

Employees need to be educated about any new policies to ensure company-wide compliance. Training sessions, workshops, and regular updates can serve this purpose. Educating employees about new policies is critical for ensuring that the entire organization adheres to compliance standards. This involves a comprehensive and sustained effort, involving multiple training formats and ongoing updates such as those listed in Table 6.7.

31 Julie Brill, "GDPR's First Anniversary: A Year of Progress in Privacy Protection," Microsoft On the Issues, May 20, 2019, https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/
32 "Full Salesforce Privacy Statement," Salesforce, July 24, 2023, https://www.salesforce.com/company/privacy/full_privacy/
33 "Annual Report," Amazon, 2022, https://s2.q4cdn.com/299287126/files/doc_financials/2023/ar/Amazon-2022-Annual-Report.pdf

Training Method	Description	Company Using Method
E-learning courses	Development of e-learning courses on GDPR compliance and data privacy, mandatory for all employees. These courses would cover handling user data, responding to data breaches, and upholding GDPR principles in daily tasks.	Cisco
Live workshops	In addition to digital courses, live workshops offer a platform for employees to ask questions and participate in scenario-based learning. These sessions could be led by internal experts or external consultants.	Google
Regular newsletters and updates	Distribution of monthly newsletters summarizing changes in data protection laws, best practices, or internal policies. These updates would help keep staff informed and current on policy changes.	IBM
Certification programs	Introduction of a certification program for roles directly involved in data processing and compliance. Certification could be a requirement for certain positions within the company.	Microsoft

Table 6.7 Training Methods and Descriptions Robust employee training works through multiple approaches.

Policy Implementation

Implementing new policies to align data handling practices with GDPR requirements turns assessment findings into actionable practices. For example, if gaps in consent management are identified, systems should be updated to ensure explicit opt-ins and proper recording of user consent. Similarly, if high-risk activities are found, the organization might introduce measures such as encryption or stricter access controls. Effective implementation often requires coordination across multiple systems and departments, ensuring that changes are consistent and integrated throughout the organization. Table 6.8 gives some examples of implementation strategies a company might use.

Implementation Strategy	Description
System-wide software updates	• Implementation of system-wide software updates to enforce new data policies, similar to Apples iOS updates that include privacy settings • Could involve changes at the user interface level, such as adding consent checkboxes and transparent data usage notifications
Back-end process overhaul	• Overhaul of back-end systems, including data storage and retrieval methods, to align with GDPR's data minimization principle • Could include modifying algorithms to anonymize user data, as seen in Google's approach to reduce privacy law violations
Employee training and change management	• Employee training sessions to ensure awareness and proper implementation of new policies • Addresses the human element of policy changes, like IBM's comprehensive training programs during major shifts in policy or technology

Table 6.8 IT Implementation Strategies and Descriptions Useful strategies for implementing new data policies include system-wide software updates, back-end process overhauls, and employee training.

Communication

Once new policies are in place, communicating these changes to end users is critical. This could occur via emails, updated terms of service, or in-app notifications, for example. Transparent and timely communication with end users is key to maintaining trust and ensuring that new policies are understood and followed. Here are three ways an organization can communicate these changes effectively:

- Email notification: An organization can distribute a comprehensive email to all users, providing an executive summary of what changes have been made in the data privacy policy, why these changes were necessary, and what users need to do, if anything, in response. The email should also provide a link to the updated full text of the policy for those who desire to review it in detail. This also includes positive receipt of notification indicating the changes to the policy have been read. An example of such a transparent approach can be found in the way Dropbox communicated its privacy policy changes in 2023.[34]
- In-app pop-up: Another effective way of ensuring the message reaches the user base is through an in-app pop-up notification. This notification can appear when users log in to the app after the policy changes have been enacted, offering them a brief overview of the changes, and directing them to more detailed information. X (formerly Twitter), for instance, employed this strategy when the company updated its terms of service in 2023.[35]
- Social media announcements: In addition to email and direct communication through the platform, leveraging other social media channels to announce changes can also be useful. A series of posts explaining the key changes in easy-to-understand language can be made on platforms such as Instagram, LinkedIn, or X to broaden the reach. Google took to its blog and social media to explain changes when the company updated its privacy policy in 2020.[36]

34 "Dropbox Terms of Service and Privacy Policy Updates," Dropbox, updated January 15, 2024, https://help.dropbox.com/security/terms-service-privacy-policy
35 X "An Update on Two-Factor Authentication Using SMS on Twitter," X Blog, February 15, 2023, https://blog.twitter.com/en_us/topics/product/2023/an-update-on-two-factor-authentication-using-sms-on-twitter
36 Sundar Pichai, "Keeping Your Private Information Private," Google: the Keyword, June 24, 2020, https://blog.google/technology/safety-security/keeping-private-information-private/

Continuous Monitoring and Auditing

Continuous monitoring and auditing are vital in ensuring that the changes implemented are not merely a one-time fix but are effectively integrated into an organization's ongoing operations. This involves conducting a mix of automated and manual reviews aimed at regularly validating an organization's compliance with GDPR. Establishing a schedule for routine audits and assessments is key, as it provides structured intervals for scrutiny, which in turn minimizes the risk of noncompliance creeping back into the organization's practices over time.

Table 6.9 describes the actions needed to monitor and audit data handling and who is responsible for each action; it also features time frames for the implementation of each task.

Action Item	Responsibility	Time Frame
1. Develop an audit framework.	Legal and compliance teams	1 to 2 months
2. Establish metrics for success.	Data analytics team, legal and compliance teams	1 month
3. Conduct quarterly internal audits.	Internal audit team	Quarterly
4. Conduct annual third-party audits.	Compliance team to select third-party auditor	Annually
5. Implement real-time monitoring systems.	IT security team	Ongoing
6. Maintain audit trails.	IT and compliance teams	Ongoing
7. Review and update policies.	Legal and compliance teams	After each audit cycle
8. Share audit outcomes.	Legal and compliance teams	After each audit

Table 6.9 Action Items, Responsible Entity, and Time Frame for Auditing GDPR Compliance Measures An example plan outlines the key action items, responsible teams, and timelines for implementing and auditing GDPR compliance measures.

Case Study: Facebook Gap Analysis, Risk Assessment, and Policy Changes

One real-world example that highlights the need for robust data security and privacy protocols involves the gaps that surfaced in the policies of Facebook (now Meta) during the Cambridge Analytica scandal. In March 2018, it was revealed that the data of around 87 million Facebook users had been harvested without consent by a third-party app and sold to Cambridge Analytica, a political consulting firm. The incident sparked global outrage, leading to intense scrutiny of Facebook's data privacy practices, and eventually resulting in significant regulatory action.

This case study explores the processes enacted during Facebook's audit, gap analysis, risk assessment, and policy development and implementation.

Facebook's approach began by identifying the scope and objectives of its audit. The focus was on how management could address the challenges and gaps in its data privacy practices to align with global standards. The scope was to examine how Facebook's failure to protect user data led to unauthorized access by Cambridge Analytica, exposing significant flaws in data management and user privacy. The primary objective was to bring Facebook's data privacy policies into compliance with global standards such as GDPR, ensuring management's responsibility for implementing necessary changes.

Facebook conducted a detailed examination of existing policies, with a critical eye toward identifying vulnerabilities and areas for improvement. Although the pre-incident policies that allowed third-party apps to access Facebook users' data were compliant with existing laws, they were found to be risky. This situation highlighted the importance of not only complying with legal requirements, but also adhering to privacy best practices to protect users' personal information.

The next phase involved comparing Facebook's practices to the stringent requirements of the EU's GDPR. GDPR emphasizes principles such as data minimization and transparency, both of which were lacking in Facebook's existing data sharing approach. The principle of **data minimization** ensures that organizations only collect, process, and store the minimum amount of personal data necessary for its purpose. Identifying specific areas where compliance with international standards was lacking underscored the need for targeted interventions.[37]

Next was the process of identifying gaps and weaknesses which involved a meticulous examination of areas where policies, procedures, and practices fell short. This step pinpointed specific areas that needed to be addressed to enhance data protection and user privacy. In the case of Facebook, the company conducted an audit and found gaps in its own user consent management, data sharing controls, and third-party data access monitoring. It then laid out a plan to address these areas systematically.

Risk evaluation considers potential negative consequences resulting from gaps and weaknesses. For Facebook, the risks included substantial regulatory fines (such as a $5 billion fine by the FTC), potential reputational damage, and the loss of user trust. For any organization, understanding these risks is essential in prioritizing and tailoring the response to ensure that the most significant threats are addressed promptly.

Based on the identified gaps and assessed risks, Facebook needed to develop clear and actionable plans to rectify its shortcomings. This included implementing changes to limit third-party access, which is access to data from an external entity to user data, enhancing user consent mechanisms, and increasing transparency regarding data usage.

The implementation phase is where planned changes are executed. Facebook, in response to heightened data privacy concerns, began to conduct more robust audits of third-party developers, enhancing oversight and adhering to stricter data privacy standards. To ensure these changes were not just one-off adjustments but part of a sustained compliance strategy, Facebook instituted continuous monitoring measures. These measures include regular reviews of data access and usage by third-party developers, the use of advanced analytics to detect and respond to unusual patterns indicative of potential data misuse, and ongoing updates to their data privacy policies and practices in line with evolving regulations and user expectations. Continuous monitoring of compliance ensures that the changes not only effectively address identified gaps, but also that ongoing compliance is maintained, adapting to new challenges and regulatory requirements as they arise.

Documenting and reporting are final steps that are vital in maintaining transparency and trust. Facebook increased transparency with users and regulators through public reports and regular updates on privacy measures, reinforcing the importance of management's role in driving these changes.

Facebook's reevaluation of its data security and privacy policies after the Cambridge Analytica scandal illustrates the process of aligning corporate practices with global standards. It also serves as a lesson for organizations to be vigilant in protecting user privacy, ensuring compliance with regulatory frameworks, and establishing transparent communication with stakeholders.

37 Colin J. Bennett, "The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?," *Information Polity* 23, no. 2 (April 2018), https://doi.org/10.3233/IP-180002

ETHICS IN IS

Ethical Considerations in Gap Analysis

In 2022, Uber faced significant backlash after a data breach exposed the personal information of millions of users. This incident underscores the ethical responsibilities companies have when managing sensitive data. The gap analysis process is not just about compliance but also about upholding ethical standards to protect user trust.

Key ethical considerations before a gap analysis include:

- Informed consent: Ensure users fully understand and agree to how their data will be used and stored.
- Transparency: Be clear and open about data collection, storage, and sharing practices.
- Trust: Protect the trust users place in your organization by implementing robust data protection measures.
- Accountability: If gaps are found, be transparent and take responsibility to address them immediately.

Ethical actions after a gap analysis include:

- Communicate clearly: Inform stakeholders promptly if any vulnerabilities are detected.
- Implement changes responsibly: Address any identified gaps with a focus on ethical responsibility, not just legal compliance.
- Ongoing monitoring: Continuously audit and monitor data practices to ensure ongoing protection and trust.

By integrating these ethical considerations into your gap analysis, the organization can enhance data security and build a culture of trust and accountability.

Key Terms

accountability principle that people and entities must take responsibility for the decisions they make and be able to explain them
action plan detailed outline of steps to be taken to achieve a particular goal, often aimed at mitigating risk or improving performance
audit process of evaluating the adequacy, effectiveness, and adherence to prescribed procedures, protocols, or standards
bad actor person or entity who hacks or cracks into a computer or system with malicious intent
California Consumer Privacy Act (CCPA) law that increases privacy rights and consumer protection for residents of California
certification body organization accredited to assess and certify the conformity of companies and organizations to specific standards, ensuring they meet the established criteria in their industry or sector
compliance adherence to laws, regulations, and policies governing an industry or operation
consent in the context of data protection, explicit permission given by an individual for the collection, processing, and use of their personal information
cyber espionage use of online methods to obtain secret or confidential information without the permission of the holder of the information, typically for strategic, military, or political advantage
data breach unauthorized access to confidential data, often leading to the exposure of sensitive information
data center facility used to house computer systems and related components, such as telecommunications and storage systems
data mapping tool software application or platform that enables data professionals to automate the process of mapping data fields, attributes, or elements from source systems to target systems or destinations
data minimization principle that organizations should only collect, process, and store the minimum amount of personal data necessary for its purpose
data privacy rights and practices around the proper collection, storage, and use of personal information
data protection impact assessment (DPIA) process to help identify and minimize the data protection risks of a project
data security protection of data from unauthorized access, corruption, or theft
digital divide gap between individuals, communities, or countries that have access to modern information and communication technologies and those that do not
error handling process in software and systems design where potential errors are systematically managed and addressed to prevent system failures and security breaches, and to provide meaningful feedback to users
gap analysis method for comparing current policies, protocols, or performance metrics against desired goals or industry standards to identify areas for improvement
General Data Protection Regulation (GDPR) comprehensive data protection law in the European Union that sets guidelines for the collection and processing of personal information of individuals within the EU
identity theft act of stealing someone's information and assuming their identity
IEEE 2413 architectural framework for IoT developed by the Institute of Electrical and Electronics Engineers (IEEE) to standardize and promote cross-domain interaction
input validation process of checking inputs received from users or from other systems for their data type, length, format, and range
Internet of Things (IoT) network that connects everyday physical objects to the internet, enabling them to collect and share data with other devices or systems
ISO/IEC 27701 extension to the ISO/IEC 27001 and ISO/IEC 27002 standards that provides guidelines for establishing, implementing, and maintaining a privacy information management system
least privilege principle cybersecurity practice where users are granted the minimum levels of access, or permissions, needed to perform their job functions, reducing the risk of unauthorized access to sensitive

information

physical security measures and systems used to protect people, property, and physical assets from external threats such as theft, vandalism, and natural disasters

policy defined guidelines and procedures established by an organization to regulate actions and ensure compliance with legal and ethical standards

Privacy by Design privacy by design concept and approach in system engineering and data handling practices that integrates privacy and data protection measures from the very beginning of the design process, rather than as an afterthought

privacy engineering incorporating privacy principles directly into the design and development of IT systems, networks, and business practices

privacy information management system (PIMS) framework or set of policies and procedures used by an organization to manage personal data and ensure compliance with privacy laws and regulations

regulatory framework structure of rules and guidelines, often legislated, within which an industry or business must operate

remote auditing modern auditing method that uses digital tools and technologies for assessing systems, processes, and policies when in-person visits are not feasible

risk assessment process of identifying potential risks that could negatively impact an organization's assets and business operations and evaluating the potential negative outcomes and the likelihood of them occurring

secure device onboarding process that involves adding devices to a network in a secure manner to prevent unauthorized access and protect the integrity of the network

social responsibility in a business context, the obligation of companies to act in ways that benefit society and the environment beyond what is legally required

third-party access ability for external entities or applications, not part of the primary institution, to access certain data or functionalities

transparency openness, communication, and accountability, wherein actions and decisions are clear and understandable to stakeholders

Summary

6.1 Key Concepts in Data Privacy and Data Security

- Data privacy and security involve protecting data from unauthorized access and ensuring confidentiality, integrity, and availability; they are essential for maintaining trust and reputation, preventing financial loss, and reducing operational risks in enterprises.
- The transition of businesses to digital platforms has increased the susceptibility of information to breaches and unauthorized disclosures, emphasizing the impact of enterprise security and risk policies on data privacy in a digital landscape.
- Data privacy and security have transcended being mere IT issues to become crucial elements of strategic planning for businesses, necessitating significant investment in data security measures and privacy protocols to maintain customer trust and comply with regulations.
- The growing awareness and concern among consumers about their data privacy means businesses must enhance their data protection efforts, as consumers are increasingly likely to switch away from companies with poor data practices.
- Security policies extend to managing risks associated with third parties such as cloud service providers and data analytics firms, requiring regular audits, and secure data handling agreements.
- Data privacy regulations and standards, both regional and international, ensure the safeguarding of personal information and provide a standardized approach for businesses to manage data privacy.

6.2 Vulnerabilities and Threats in Web Applications and IoT Technology

- The rapid advancement of digital technologies, including IoT and mobile, has introduced significant vulnerabilities.
- The expansion of IoT and web applications has integrated technology into every facet of modern life, increasing the responsibility of enterprises and IT professionals to ethically manage and secure these interconnected ecosystems.
- Security strategies include both preventive and reactive measures intended to combat security threats in web and IoT technologies, preparing future IT professionals to effectively protect digital environments.
- Regulatory frameworks and standards developed by organizations such as ISO and IEEE are essential for enhancing security, interoperability, and quality in the digital ecosystem, particularly in the underregulated IoT sector and its global reach.

6.3 Data Security and Privacy from a Global Perspective

- The ISO/IEC 27001 standard is a key global framework for data security and privacy. It serves as an international regulation that sets specific requirements for information security management systems (ISMSs).
- The global landscape of data security and privacy is a combination of intricate regulations, standards, and best practices that reflects the diverse concerns of different regions and industries. It is in a perpetual state of evolution.
- Some of the most well-known standards are the globally recognized COBIT 2019 Framework, the Enterprise Privacy Risk Management Framework, ISO/IEC 27701, and the NIST Privacy Framework.
- While the United States has put in place various agencies and standards to oversee data protection, other countries across Asia, South America, Africa, as well as various industries have crafted similar frameworks to safeguard user information.
- The case study provides important insights on the strategic importance of global certifications, the need for flexibility, and the value of expert auditors in navigating global regulations and frameworks.

6.4 Managing Enterprise Risk and Compliance

- Enterprises can significantly benefit from conducting an audit and gap analysis to determine compliance with global frameworks, a critical process that helps identify discrepancies between current data security and privacy practices and industry-wide best practices or regulatory requirements. A gap analysis is invaluable for pinpointing areas where policies may leave the company or its users' data vulnerable to various risks.
- Introducing new data privacy and protection policies is a critical step for any organization aiming for GDPR compliance. These policies undergo a thorough legal review to ensure they meet GDPR standards and are also vetted internally across various departments to check for operational feasibility and effectiveness.
- To ensure company-wide compliance, it's essential to conduct comprehensive employee training on new data protection policies. This involves a mix of e-learning courses, live workshops, regular updates, and, for certain roles, specific certification programs to ensure that every member of the organization understands and can effectively apply these policies.
- Continuous improvement is key in GDPR compliance, which involves regular policy reviews, automated compliance monitoring, and audits. Equally important is transparent and effective communication with end users regarding any policy changes to maintain trust and compliance.

Review Questions

1. What is a description of Privacy by Design?
   a. a principle advocating for privacy to be intentionally embedded into the design and architecture of IT systems and business practices
   b. a principle focusing on the technical aspects of implementing data protection controls, such as

encryption and anonymization
- **c.** a principle focusing only on data storage and management by third-party providers
- **d.** a principle that is reactive to data protection and is only considered after a data breach has occurred

2. The General Data Protection Regulation (GDPR) impacts ________.
- **a.** only organizations based in the EU
- **b.** only organizations based outside of the EU
- **c.** all organizations that process the data of EU citizens, regardless of the company's location
- **d.** only organizations that have a physical presence in the EU

3. The International Organization for Standardization's (ISO) 27701 standard is an extension of ISO 27001. What does ISO 27701 provide guidance on?
- **a.** how to manage privacy information
- **b.** how to manage third-party relationships in data storage
- **c.** how to create new data privacy laws
- **d.** how to design privacy into IT systems and business practices

4. How did internet usage change from the 1990s to the 2020s?
- **a.** It decreased due to privacy concerns.
- **b.** It increased slightly with the growth of technology.
- **c.** It skyrocketed due to the rise of big data and digital lifestyle.
- **d.** It remained stable as internet penetration rates reached a plateau.

5. What is the term for the practice of incorporating privacy controls into the design and development of IT, systems, networks, and business practices?
- **a.** Privacy by Design
- **b.** privacy engineering
- **c.** security engineering
- **d.** privacy network

6. What kind of attack exploits vulnerabilities in a web application to inject malicious scripts into websites viewed by other users?
- **a.** man-in-the-middle attack
- **b.** SQL injection
- **c.** cross-site scripting
- **d.** phishing

7. Which attack can turn unsecured IoT devices into bots to carry out massive, distributed denial-of-service (DDoS) attacks?
- **a.** Mirai botnet attack
- **b.** SQL injection
- **c.** CSRF attack
- **d.** dictionary attack

8. Which international standard provides a framework for an information security management system (ISMS)?
- **a.** ISO 31000
- **b.** ISO/IEC 27001
- **c.** ISO 9001
- **d.** ISO 14001

9. When developing web and IoT technologies, enterprises and IT professionals have the social responsibility to ________.
- **a.** maximize profit

b. ensure user engagement
c. safeguard user information and privacy
d. minimize development costs

10. Which regulation enacted by the European Union focuses primarily on data protection and control?
    a. COPPA
    b. GDPR
    c. CCPA
    d. LGPD

11. Which organization has been heavily involved in developing standards specifically for IoT?
    a. W3C
    b. IEEE
    c. ITU
    d. NIST

12. In the case study, what was the primary reason behind the Texas-based data center efforts to gain ISO/IEC 27001 certification?
    a. legal requirement
    b. client demands
    c. strategic business decision
    d. government grants

13. Which type of organization would most likely require that its data centers be ISO/IEC 27001 certified?
    a. local shops
    b. Fortune 500 companies
    c. small online businesses
    d. individual clients

14. What is a primary focus of a gap analysis related to data security and privacy?
    a. identifying strong performance areas only
    b. assessing whether the organization's philanthropic efforts are successful
    c. comparing current policies against industry standards to identify weaknesses
    d. measuring the CEO's leadership skills

15. In terms of compliance with global frameworks such as GDPR, what principle emphasizes collecting only the data strictly necessary for intended purposes?
    a. data maximization
    b. transparency
    c. data minimization
    d. data expansion

16. What is the main objective of conducting an audit in the context of data security and privacy?
    a. to hire new staff
    b. to align an organization's practices with global privacy standards
    c. to redesign the company's organizational structure
    d. to evaluate employee performance

17. In complying with global frameworks such as GDPR, what does the term *transparency* primarily refer to?
    a. the organization's revenue
    b. clarity in how user data are used and managed
    c. the physical layout of an office
    d. government operations

18. Which of the following would be considered a significant risk associated with gaps in data security policies?
    a. reduced employee turnover
    b. increased stock prices
    c. loss of user trust and potential regulatory fines
    d. introduction of new company products

19. The scope of a gap analysis for data security and privacy usually includes evaluating ________.
    a. employee behavior and data sharing controls
    b. third-party data access and customer behavior
    c. evaluating areas such as user consent management, data sharing controls, and third-party data access
    d. consent management only

Check Your Understanding Questions

1. Briefly explain the differences between Privacy by Design and privacy engineering. How do these concepts play a role in enterprise security and risk policies?

2. The GDPR and the CCPA are two major data privacy regulations implemented in the European Union and California, respectively. What are the key rights these regulations provide to individuals, and what are their implications for businesses?

3. What are some of the key drivers behind the rapid data creation in our current digital age, and how has this impacted data privacy and security?

4. Discuss the international dimensions of data privacy. Why is it essential for businesses to understand varying privacy regulations and practices in different regions?

5. What is one major vulnerability commonly found in Internet of Things (IoT) devices, and how has this vulnerability been exploited in a real-world example?

6. Describe one specific regulation or standard (such as GDPR or ISO/IEC 27001) aimed at enhancing the security and privacy of web and IoT technology.

7. How do regulations such as GDPR and CCPA impact the social responsibility of enterprises and IT professionals developing web and IoT technology?

8. What is one future challenge that may require reevaluation of existing regulations and the creation of new guidelines or regulations for web and IoT technology?

9. Briefly explain the importance of an information security management system (ISMS) in the context of data security and privacy.

10. List at least two regulations that impact data security and privacy in countries outside of the United States.

11. Briefly explain what a gap analysis is and how it helps in enhancing an organization’s data security and privacy.

12. What are some key principles of the General Data Protection Regulation (GDPR) that organizations should comply with?

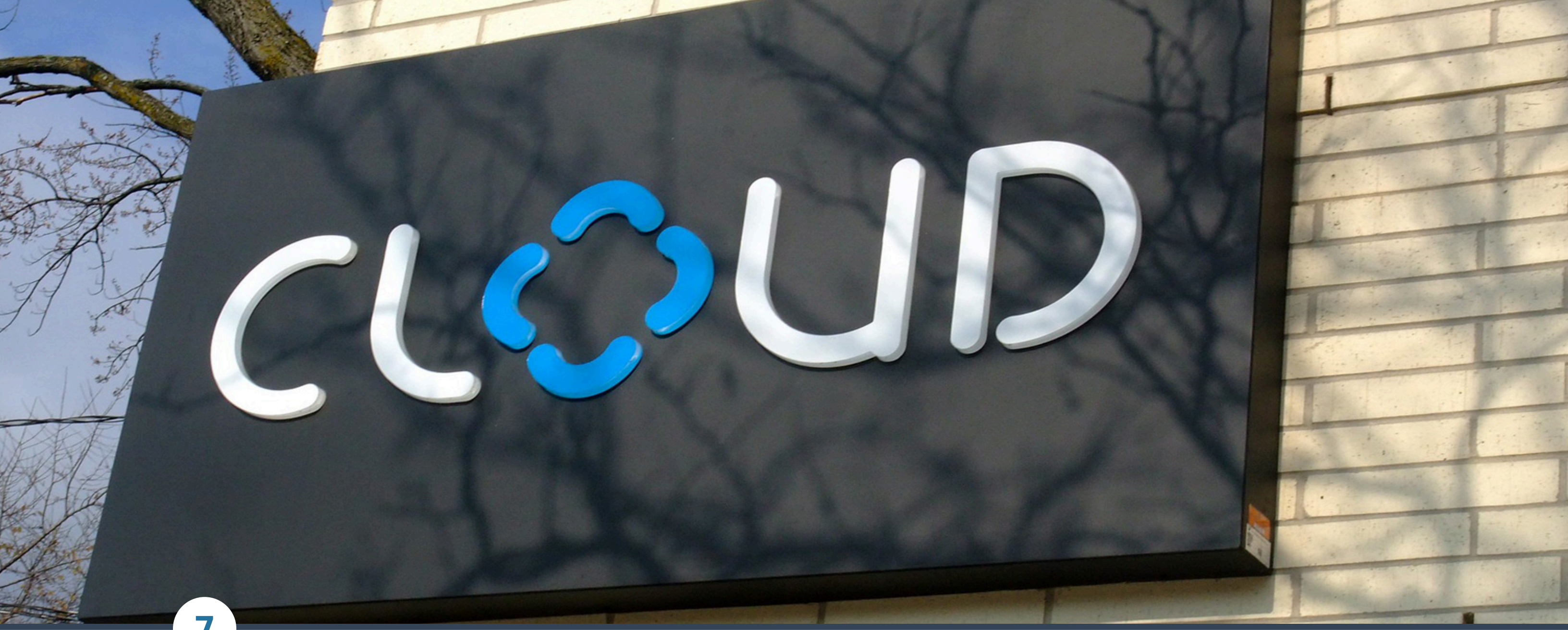
13. Describe some potential risks that organizations could face due to gaps in their data security and privacy policies. How could an organization mitigate these risks?

Application Questions

1. Reflect on the importance of data privacy and protection in today’s increasingly digital world. How do you see these concerns influencing your personal habits online and your future professional life, particularly if

you are considering a career in information systems? How do you believe businesses and regulations need to evolve to maintain data privacy and protection in the face of rapidly changing technology?

2. Watch Glenn Greenwald's "Why Privacy Matters" TEDx talk (https://openstax.org/r/109TEDGreenwald) and answer the following question: How does Greenwald's perspective on the importance of privacy align or contrast with the ideas presented in the text about the role of data privacy and security in the digital age? Provide specific examples from both the video and the text in your response.
3. Reflect on the ethical responsibilities of IT professionals in shaping the use and development of web and IoT technologies. Do you think IT professionals should have a moral duty to be socially responsible, particularly in ensuring user privacy and security? How do their roles and actions influence the broader regulatory and ethical landscape?
4. Considering the increasing interconnectedness of our world through IoT, what are some sectors or industries that you believe will face the most significant regulatory challenges in the future?
5. Watch this video about hackers remotely hijacking a vehicle (https://openstax.org/r/109RemoteHijack) and answer the following questions: Given the increasing connectivity in modern vehicles, what implications does the hacking of a vehicle with the driver inside have for consumer trust and automotive cybersecurity? While this incident occurred with a specific make and model, any vehicle could have been affected. How do you think regulations and guidelines can address such vulnerabilities?
6. Consider the various strategies and best practices for protecting an organization from a ransomware attack. As a leader in the IT industry, how would you proactively prepare and safeguard your organization's digital assets and data against such an attack?
7. Reflect on how an information security management system (ISMS) could benefit an international organization or national organization that you are familiar with. What specific challenges and opportunities can you identify for implementing an ISMS in this organization?
8. Watch this video by Rachel Cummings on the Data Privacy Index (https://openstax.org/r/109DataPrivIndx) and consider the following: How can an index such as a FICO score used by credit card companies and banks be used across various social media platforms and rideshare platforms such as Lyft, Uber, TaskRabbit, or AirBnB? What are the limitations?
9. Reflect on a recent news event involving a data breach or data privacy scandal. How do you think a gap analysis could have prevented or mitigated the issues at hand?
10. Think about your own experiences with online services and their privacy policies. Are there any instances where you felt that a service could improve its data security or privacy policies? What specific gaps did you identify and how would you address them?



7 Cloud Computing and Managing the Cloud Infrastructure

Figure 7.1 Cloud computing and the development of cloud infrastructure are critical to delivering software applications securely, more rapidly, and continuously. (credit: modification of work "Cloud" by James Cridland/Flickr, CC BY 2.0)

Chapter Outline

Introduction

Organizations are facing more pressure today to retain customers who depend on updated or new business capabilities. This requires organizations to deliver software applications securely, more rapidly, and continuously. For organizations to adapt existing applications or build new applications using the cloud, they must abide by a different set of constraints to leverage cloud infrastructure in comparison to traditional on-premise infrastructure.

Cloud computing offers the ability to access information via the internet at any time of day, from any device, and from any location. Before the cloud existed, transferring large amounts of data required physical external storage devices. The limitation of carrying data on a physical drive meant that employees could not work remotely and maintain access to all necessary information when away from the office. There was also not yet a means for customers to access banking information from an app, to shop online from a laptop, or to write an essay using Google Docs from a desktop computer. Cloud computing changed all of that, and it enriched the depth and breadth of information systems (IS) development and efficacy in the modern business world.

7.1 Fundamentals of Cloud Computing

Learning Objectives

By the end of this section, you will be able to:

- Define cloud computing and its relevance to the organization
- Compare and contrast cloud computing and in-house hosting
- Discuss the role of information systems professionals in cloud computing

The application of cloud computing offers businesses the ability to add, expand, or modify systems to be used in accounting, human resources, and daily operations. Consider Google Drive, for example, which a user can access from their smartphone to create and save a document. That user can then allow another user to access and modify that document from another device. Google Docs also allows multiple people to work together within the same document at the same time. Such advantages give cloud computing the ability to help an organization work more effectively and efficiently.

Cloud Computing and Its Relevance to the Organization

Consider a situation in which an organization is faced with the need to rapidly expand a new product line, which could increase the company's competitive advantage in their industry. What is the timeline to purchase physical equipment and install, configure, implement, and support the needed resources, including human resources? Depending on the organization's purchasing requirements, it could be a minimum of thirty days to push a purchase order through, if funding is available. Depending on the amount of equipment ordered, delivery may take forty-five to sixty days or more. Once the equipment is received, there is the configuration and implementation aspect of the project. This step depends on the abilities of the staff and whether there are special application requirements, testing, or piloting of the resources.

Take the same project and consider how it may look different if it is planned and executed in the context of **cloud computing**, often referred to simply as "the cloud," which is information technology (IT) resources that are available through the internet on an on-demand or pay-as-you-go basis without the users needing to manage it. The organization would need a **cloud provider**, a company that provides on-demand services such as data storage, applications, and infrastructure in a platform accessible through the internet. Once the organization has a cloud provider, it then becomes a **cloud consumer**, which is an entity that uses and maintains access to the computing resources of a cloud provider. The organization can use the cloud provider's portal to order, build, configure, and implement the needed **infrastructure**, which is the facility and system used to support an organization's operations. The organization can then use a portal to complete the same build, configuration, software installation, testing, and piloting to be accomplished in the physical environment (Figure 7.2).

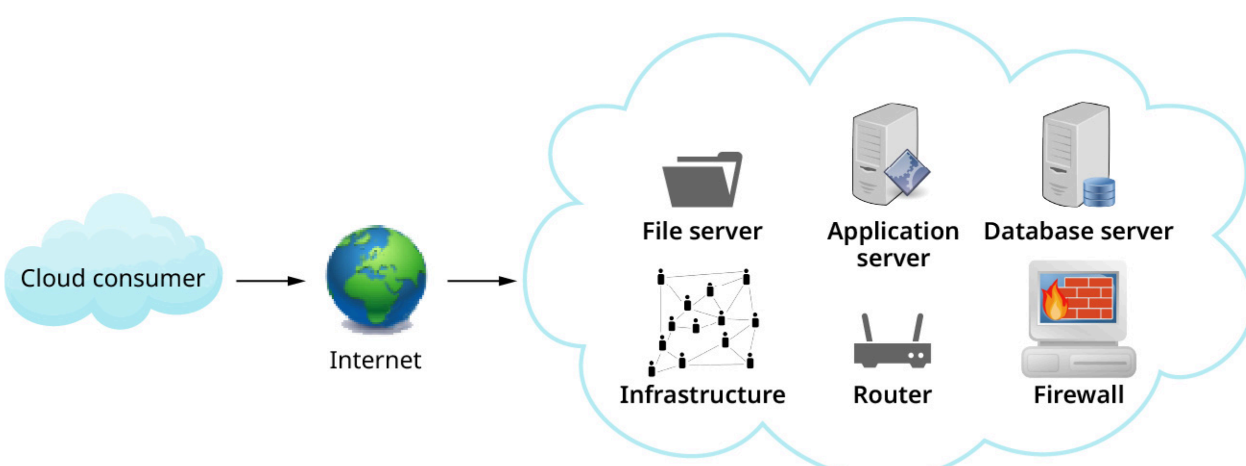


Figure 7.2 A cloud-based environment connects a cloud consumer to cloud components like servers and firewalls via the internet.

(attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit “File server”: modification of work “Simpleicons Interface folder-open-shape” by SimpleIcon/Wikimedia Commons, CC BY 3.0; credit “Application server”: modification of work “Application Server” by Openclipart/Wikimedia Commons, Public Domain; credit “Database Server”: modification of work “Database Server” by Openclipart/Wikimedia Commons, Public Domain; credit “Infrastructure”: modification of work “Network (22612) – The Noun Project by Ann Fandrey/Wikimedia Commons, CC0 1.0; credit “Router”: modification of work “Router (16624) – The Noun Project” by Christopher Pond/Wikimedia Commons, CC0 1.0; credit “Firewall”: modification of work “Firewall (computing)” by Openclipart/Wikimedia Commons, Public Domain)

The organization will need to determine the competitive advantage of each approach to expanding to a new product line. It might take several months if the organization decides to use their own infrastructure to implement an **on-premise environment**, which is the physical hardware, such as servers, network equipment, and workstations. The cost of that implementation could occur concurrently to the rollout of a new product line that the system will support, thus maximizing the capital expenditure for the project (Figure 7.3). The cloud scenario, which could be implemented in days rather than months, might meet the immediate needs of a new project that must adhere to specific deadlines that do not offer an extended amount of start-up time.

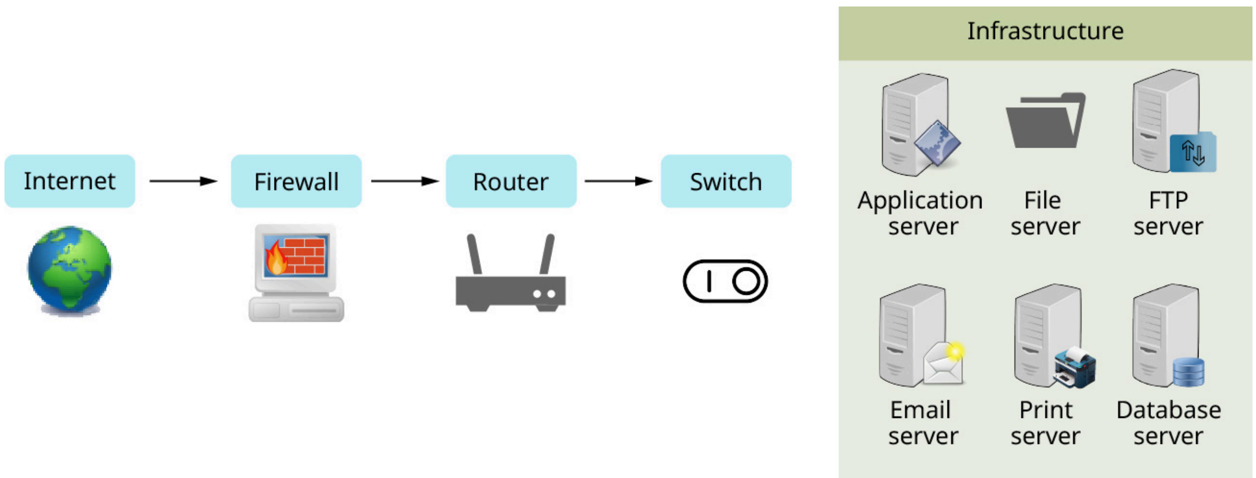


Figure 7.3 An on-premise environment is connected to the internet through a firewall, and network traffic passes through a router and switch. The infrastructure consists of application, file, FTP, email, print, and database servers. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit "Firewall": modification of work “Firewall (computing)” by Openclipart/Wikimedia Commons, Public Domain; credit "Router": modification of work "Router (16624) - The Noun Project" by Christopher Pond/Wikimedia Commons, CC0 1.0; credit "Switch": modification of work "Noun Project switch icon" by "IconMark"/Wikimedia Commons, CC BY 3.0; credit "Application server": modification of work "Application server" by Openclipart/Wikimedia Commons, Public Domain; credit "File server": modification of work “Simpleicons Interface folder-open-shape” by SimpleIcon/Wikimedia Commons, CC BY 3.0; credit "FTP server" and "Database server": modification of work “Database Server” by Openclipart/Wikimedia Commons, Public Domain; credit "Email server": modification of work "E-mail-server" by Openclipart/Wikimedia Commons, Public Domain; credit "Print server": modification of work "Fax server" by Openclipart/Wikimedia Commons, Public Domain)

Cloud computing environments and on-premise environments have the same functionality, but they have some fundamental differences. One main difference is the physical environment. In an on-premise facility, an organization owns and manages their own infrastructure. In a cloud environment, the cloud provider owns, operates, and manages the computing equipment. Both computing environments have a physical hardware component, yet the cloud environment offers services to the cloud consumers using **virtualization**, in which a physical computer environment creates a simulated computer environment (Figure 7.4). Virtualization software takes physical hardware, such as a server, and converts it to resources that are then reallocated through code to re-create an IT resource that functions in the same manner as the physical equivalent.

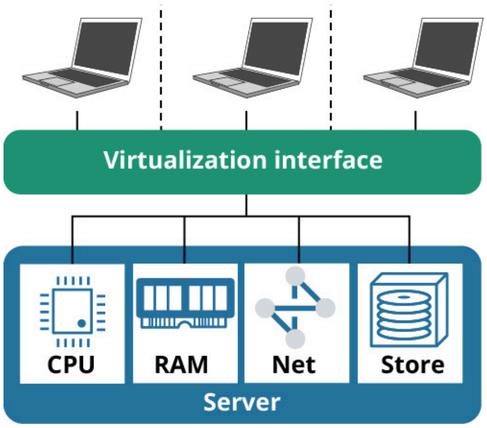


Figure 7.4 An interface virtualizes the resources, such as CPUs, RAM, network, and, in some cases, storage, of the physical server. It divides these resources while allocating what is needed for each computer accessing the server. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

In an on-premise environment, the organization provides access to the different platforms, such as Exchange, file, and database, and applications, such as email, the web, and data entry. Access to the internet occurs through the on-premise network infrastructure and is monitored and maintained by the organization.

In a cloud environment, the cloud provider owns and manages physical hardware to deliver virtualized access through the internet to the server, network equipment, and workstations. The cloud environment can support access via any device, from any location, at any time based on the contracted services the cloud consumer purchases. For example, a cloud environment in a school allows a student to review their grades at any time. The student can use their smartphone to access the school portal, and with the correct credentials, they can log in and access the platform that houses their grades.

Cloud environments are based on the services the cloud provider offers to the cloud consumer. Amazon Web Services (also known as AWS or AWS Marketplace) provides many services based on the categories the cloud consumer procures. Some of the service categories are operating systems, security, networking, and storage.

Though companies, such as AWS, Google, and Microsoft Azure, offer a wide range of services, some cloud environments specialize in services that meet a single requirement for a cloud consumer. One example of a single service is a development environment, such as those provided by DigitalOcean. This environment allows developers to build a web and application platform that can be scaled to their needs and can run independently from their production environment.

Data storage is a problem that all organizations face—from how much they create to how long they should retain it. The amount of data generated is relevant to their customer base, products, and services. This, in turn, creates an issue with determining the amount of storage required at any given time. Cloud storage offers organizations the opportunity to implement accessible **elastic storage**, meaning that it can expand or collapse based on demand. Cloud providers such as Wasabi Technologies (also known as Wasabi) specialize in offering only storage environments, such as hot site storage, network-attached storage, and data lakes. In **hot site storage**, mission-critical data are stored in one location where the organization can have immediate access to the data. In **network-attached storage (NAS)**, the storage system is flexible and attaches to an organization’s network infrastructure. In a data lake, large amounts of structured and unstructured data are stored in a repository.

Cloud Computing Compared to On-Premises Hosting

There are several advantages and disadvantages of cloud computing. First, consider the difference between an organization that has on-premise equipment and one that uses a cloud computing environment. Each organization has data storage, website hosting, and system availability for an **end user**, or the entity that makes use of the technology provided by an organization.

When organizations have their own equipment to provide the services to their end users on-premise, the organization manages, maintains, and supports all services in-house. These services are dependent on the services the organization provides to their customers and the industry in which they operate. The support of these services includes, but is not limited to, the facility, utilities, hardware, software, and other equipment necessary to perform the functions the end users need to complete their job function. In most cases, the company has its own personnel to support the equipment and services necessary to support the technology and systems the organization operates, such as Active Directory services, website development, and data storage.

In cloud computing, the resources are located external to the organization's facilities and accessed through the internet. According to the National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] According to this definition, there are five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service; three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS); and four deployment models: community cloud, private cloud, public cloud, and hybrid cloud[2] (Figure 7.5).

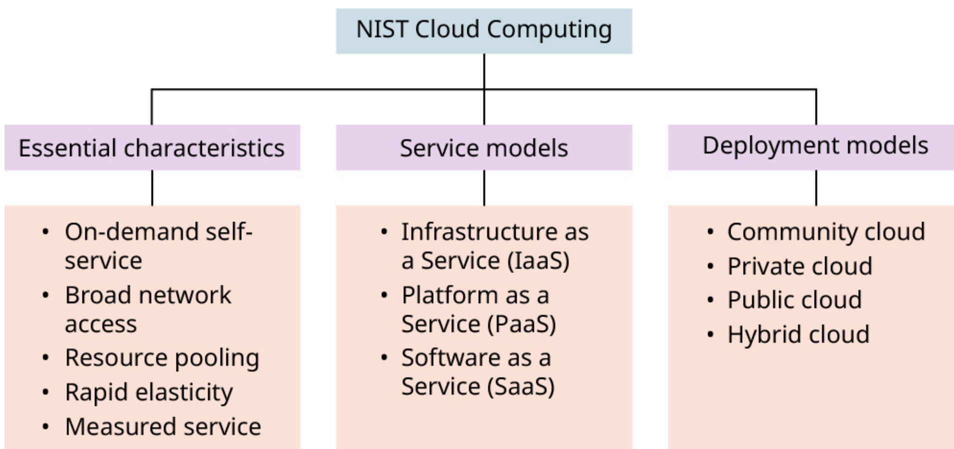


Figure 7.5 The NIST Cloud Computing Model is composed of five essential characteristics, three service models, and four deployment models. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Cloud computing infrastructure is based on a physical environment that uses virtualization technology to expand the capabilities of the physical equipment. Virtualization offers the cloud environment **scalability**, which is the ability of the resource to be scaled up or down with minimal effort, as well as flexibility, access to system resources, and a cost factor based on services that are contracted. The process of virtualization requires a platform to operate the virtual infrastructure, another platform that creates the virtual environment, and a service to manage the virtualized resources.

There are many server virtualization software companies, such as VMware, Microsoft, SUSE Linux, and Citrix. Each server virtualization software package offers different features (such as resource allocation, high availability, and centralized management) based on the cloud environment that is to be created according to the cloud consumer's needs.

1 NIST Cloud Computing Standards Roadmap Working Group, "The NIST Definition of Cloud Computing," in *NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291, Version* 2, National Institute of Standards and Technology, July 2013, https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf, 2.
2 NIST Cloud Computing Standards Roadmap Working Group, "The NIST Definition of Cloud Computing," in *NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291, Version* 2, National Institute of Standards and Technology, July 2013, https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf.

FUTURE TECHNOLOGY

Cloud Computing and Generative AI

Cloud computing has a solid place in the computing world, which has led to new applications for hybrid clouds, multicloud environments, and now, generative AI. Cloud providers can integrate generative AI into their platforms, providing AI-as-a-Service and thereby making it more accessible and usable for organizations. Having generative AI as part of a cloud provider's platform allows an organization the flexibility to use it in many different applications, such as content creation, data analysis, and more. Cloud infrastructure will continue to scale and optimize to support the massive computational demands of training and running generative AI models, allowing businesses to focus on leveraging generative AI without worrying about underlying technical details. Further, the accessibility of generative AI in cloud computing can help promote innovation, especially in fields that previously may not have had access to the technology. The future of cloud computing and generative AI is a dynamic, evolving landscape that promises to revolutionize industries, increase accessibility, and drive innovation. With advancements in scalability, cost-efficiency, AI ethics, and automation, cloud environments will continue to serve as the foundation for generative AI technologies, making it easier and more powerful for organizations to leverage AI in creative and transformative ways.

The Role of Information Systems Professionals in Cloud Computing

The cloud network infrastructure has evolved from the traditional physical network to software-defined networks. A **software-defined network (SDN)** is a network that uses software for traffic management in programmable controllers and interfaces. The evolution to SDNs means that the roles and specialties of IS professionals have also evolved. Network engineering**,** systems administration, and cybersecurity are a few of the important specialties involved in cloud computing. A **network engineer** is the person with the skill to design, implement, and manage a network in support of an organization's mission. They will need to understand not only networking principles but also virtualization, coding languages (such as Java, JavaScript, and Python), and server administration. The **system administrator** is the person who manages and maintains the IT and IS resources for an organization. They will need to handle server administration, and they will also have to know the different operating systems and the virtualization system management interfaces. An operating system (OS) is the software installed on a computer system, such as Windows, Linux, or Unix, that manages the resources. The system administrator will need to be proficient in server virtualization software, coding languages, and platform-specific applications.

A **cybersecurity specialist** is a person who identifies and develops security strategies, verifies needed security improvements, and implements security strategies for an organization. This position needs a person who can recognize the possible risks that an organization might encounter. People pursuing cybersecurity need to understand cyber threats, and they will also need to know networking, system operations, physical security, and information security. According to the U.S. Bureau of Labor Statistics, cybersecurity positions should grow 33 percent between 2023 and 2033.[3]

CAREERS IN IS

Cloud Computing Employment

There are many career opportunities in the field of cloud computing. The types of jobs that are available range from network engineers, who manage networks, to software developers, who maintain IS and IT

3 Bureau of Labor Statistics, "Information Security Analysts," *Occupational Outlook Handbook*, U.S. Department of Labor, last modified August 29, 2024, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

resources, to cybersecurity specialists, who develop security strategies. Individual employers have different requirements for the type of IS personnel they need, so even after choosing a specialty and earning a degree, you may need additional education, certifications, or experience. Certification requirements may include those related to specific software or hardware manufacturers. Because of the nature of the specialties in the field of cloud computing, it is important to research employers' requirements to ensure you have the qualifications they are seeking.

Case Study: Using the Cloud to Prepare for a Natural Disaster

When dealing with IT resources, anything can change how a company does business. Consider the city of Houston, Texas, which must be prepared for a natural disaster, such as a hurricane. As a result of hurricanes that have affected Texas in the past, the state government has had to shut down, and employees have had to relocate. In such a scenario, the concern becomes how to serve the citizens of Texas who depend on the state for their benefits. With employees and clients relocated, it becomes more complicated for the state to provide services with locally maintained databases and client information. The state can take a wait-and-see approach and delay services until the data centers become operational again. Another option might be for the state to acquire new IT resources and set up new data centers in an area less prone to hurricanes, which takes time, funds, personnel, and additional facilities. A third option might be for the state to transition to a cloud-based environment, which will take time to develop, implement, and roll out. The time constraints and cost factors for the third option are significantly less, and the need for a facility is nullified. The state government will need to evaluate and justify each option, based on the criticality of the state's operational needs and the needs of the clients.

All three scenarios meet the organization's needs, so the justification process will involve the availability of funds, personnel, and facilities. A major portion of the justification will be to consider the time frame the organization needs to return to an operational status. With a wait-and-see approach, there is no planning for how long it will take to return to normal operations. The time frame needed for an on-premise resource environment to return to normal operations is based on the availability of the needed resources, delivery timelines, qualified personnel, and facilities. The time frame needed for a cloud-based resource environment to return to normal operations is usually shorter and may be days instead of weeks or months. The funds needed for an on-premise environment are usually greater than those of the cloud-based environment, and depending on the funding structure of the organizations, a lower-cost solution may be approved without major effort.

With the introduction of cloud-based resources, organizations now have a new component to add to their tools for IS operations. The concept of IS operations requires an organization to make allowances and plans for downtime scenarios. One course of action is **business continuity**, which is a plan that an organization puts in place to maintain its operational status in an emergency scenario. The plan requires the company to inventory its IS resources, validate the requirements for its users, and develop a plan to address the needs should an outage occur. The plan would provide details for how the outage is to be handled, who is involved to assist in the outage, and what steps should be taken to restore services.

The other course of action is plans for **disaster recovery**, the process an organization follows to reestablish operational status after an incident causes a system failure. This plan is more detailed than the business continuity plan, yet it uses some of the same information as the business continuity plan. The difference between the two plans is that the disaster recovery plan takes into account a system failure that prevents operations at a large scale. For example, a network outage would fall under business continuity, whereas the crash of a database server could be classified as disaster recovery if there is not a backup database server.

The cloud-based environment offers companies additional options for doing business on a regular basis and in an emergency transition scenario. It provides the organization with a methodology for designing new resources, implementing new resources, or even creating a resource environment to use in business continuity and disaster recovery that includes business impact analysis and incident handling processes.

7.2 Cloud Computing Services, Pricing, and Deployment Models

Learning Objectives

By the end of this section, you will be able to:

- Discuss how cloud services are delivered and priced
- Identify major cloud service providers and their delivery models

Delivery models that service providers use to support the cloud consumer vary based on the needs of the cloud consumer. Advances in technology and the growth of the cloud environment have led to the development of new service models. Each evolution in technology offers advancements in service deliverables that the cloud provider can offer cloud consumers. Today's cloud environment is much different from the earliest version when operations began to move to the cloud.

Cloud consumers now have many options for choosing a hosting platform when pursuing a move, transformation, or implementation of a cloud platform for their organization. The cost for the platform is one of the factors that an organization will consider when determining whether the cloud solution is the technology the organization needs to gain a competitive advantage. Each organization has different technology requirements, and the cloud provides an opportunity for the organizations to challenge themselves to move with innovation.

Deployment and Pricing of Cloud Services

Cloud services are provided using a **delivery model**, which includes the resources offered by the cloud provider, and a **deployment model**, which includes the location, the method, and the entity responsible for controlling the infrastructure. The primary delivery models are broken down into Infrastructure as a Service, Platform as a Service, and Software as a Service. The **Infrastructure as a Service (IaaS)** model involves the provision of infrastructure resources, such as networking and storage. The **Platform as a Service (PaaS)** model manages the software and hardware resources for the purpose of development. **Software as a Service (SaaS)** is the delivery of applications in the cloud. Each of the delivery models has a specific function when it comes to building cloud services, but they are all subscription-based processes of delivering infrastructure, network, and applications, which is why they are all considered "as a Service." All three delivery models are scalable up or down, and are available on-demand to the cloud consumer. The delivery models are built on top of each other in a layered approach to building the cloud environment. The other factors in a cloud environment that are customizable for cloud consumers are the specifications, such as processing power, RAM, storage, and applications.

Infrastructure as a Service is the first level of the cloud environment that must be designed based on the requirements of the cloud consumer. This service can include, but is not limited to, raw IT resources, such as compute resources, which include the specific operating systems, the hardware components, and the network systems, such as connectivity. The functionality of the IaaS environment provides the needed control over the cloud structure while also providing the cloud consumer the ability to configure and utilize the IaaS functionality to its fullest. The IaaS environment consists of the virtual server, which is leased through the cloud provider based on memory, the CPU, and storage.

Platform as a Service is typically the second level of the cloud environment and is built in relation to the IaaS component. This service is a preconfigured environment that supports a cloud consumer's operational needs. The PaaS delivery model can be as simple as file services, such as storage of data files on a file server, or as complex as database services with business intelligence used for business analysis. This portion of the delivery model requires the cloud consumer to identify specific tasks that are associated with their operational requirements, such as extending an existing on-premise resource by creating a secondary backup system in the cloud, or replacing an existing IS. The PaaS offers the cloud consumer the opportunity to configure the prebuilt environments and removes some of the complexity involved in configuring an IaaS environment with a **bare metal server**, which is a physical server deployed for a single customer that provides the customer full access to the server resources.

Software as a Service offers a wide range of available products to cloud consumers, which embodies the essence of cloud computing: to make as many services as possible available to as many consumers as possible. A wide range of products exist in the cloud computing environment. Depending on the product, cloud providers can offer leases for the use of different services on different terms based on the needs of the cloud consumer. Figure 7.6 shows all three levels of delivery models.

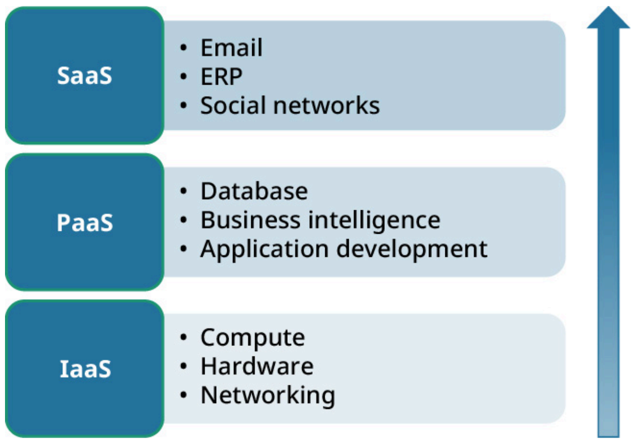


Figure 7.6 The base level of the cloud environment is IaaS, the second is PaaS, and the top is SaaS. Each level stacks on the one below it so that they work together to form the foundation and ultimately enable the cloud consumer to build, develop, and deploy the software applications they need to operate. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

As the availability of newer technologies has grown and evolved (processors with more cores, faster GPUs), cloud providers have gained access to many new offerings. These offerings have changed the possibilities for the cloud consumer when it comes to adding their cloud environment. Some of these new offerings are **Database as a Service (DBaaS)**, which is a service that gives cloud consumers the ability to manage and maintain relational and nonrelational databases; **Communication as a Service (CaaS)**, which is a service that allows for the cloud-based delivery of services such as Voice over Internet Protocol, videoconferencing, and internet-based telecommunication services; and **Testing as a Service (TaaS)**, which is a service that cloud providers have built to outsource testing of software, applications, and other components that would normally be performed within the organization.

Each of the delivery models has components that are subject to a contract requirement that is supported with a **service-level agreement (SLA)**, a document that outlines the levels of service that a cloud provider assures the cloud consumer they will receive. The SLA is used as a point of reference for the daily operation of a cloud consumer's environment. Each cloud provider has a monitoring tool in place to determine the level of service provided, and there are often penalties listed in the SLA that can apply if the cloud provider fails to meet the required levels of service.

The cloud provider will establish the usage parameters in the contract for billing purposes. The usage parameters are needed to determine the cost of the cloud-based services. The services range in cost based on the usage by the cloud consumer as they pertain to the infrastructure, platform, and software requirements. A usage charge is usually calculated per hour based on the service, and the cloud consumer will incur additional charges if the usage level is exceeded. An example of this would be a per-hour charge for the service with a set number of transactions. Once the number of transactions is reached, there will be an additional transaction charge, which may be per transaction or may be a tiered amount for a certain number of additional transactions.

Each service that is offered has a predetermined rate, which is calculated based on the cloud consumer's location. The rates are charged on a 24/7 basis as outlined in the cloud consumer's contract. The rates may change based on the locations of the cloud-based environment and which location or locations the consumer uses. For example, the IaaS may be located in San Antonio, Texas, and the PaaS is located in Seattle, Washington, and the SaaS is located in Boston, Massachusetts. Cloud-based services may also be located globally, so the cloud consumer can use all the U.S.-based sites for their basic delivery models and have their backup run to Singapore.

There are four major cloud deployment models: **community cloud**, an infrastructure shared by multiple organizations with a common interest; **private cloud**, an infrastructure dedicated to a single organization; **public cloud**, an infrastructure that provides services in an on-demand environment; and **hybrid cloud**, a combination of the public and private models that can be combined with on-premise infrastructure. Each of the models is deployed based on the access needs, who is to be the owner of the environment, and the size of the environment.

A community cloud environment is one that is owned by a specific community or a cloud provider that is offering services to that community (Figure 7.7). Access to the community cloud is limited to the community that built and manages the cloud environment, such as a university with multiple campuses or a firm with multiple office locations. Membership is granted to those outside the community at the discretion of the community, and access is controlled by the community. Since community clouds are shared by organizations in the same industry, those that do business in a certain sector, such as education, must adhere to certain sector-specific regulations for their entire cloud.

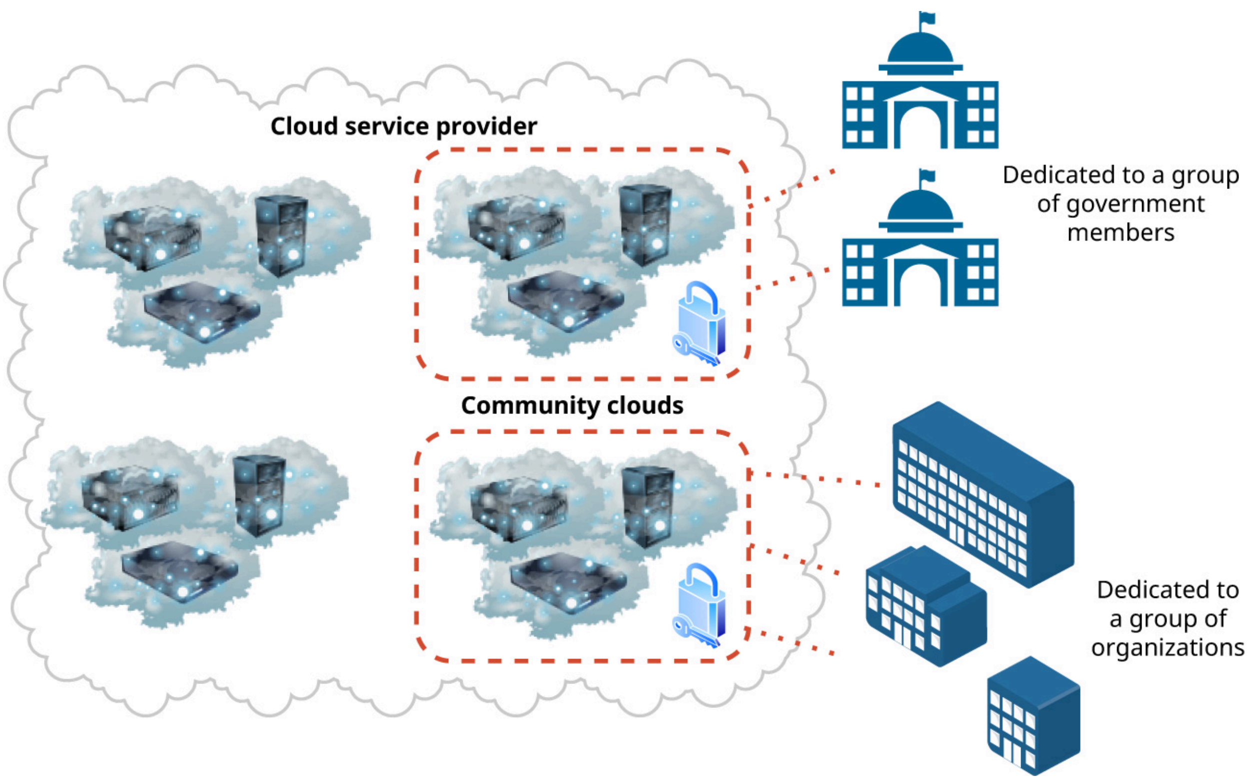


Figure 7.7 The structure of a community cloud is dependent on the requirements of the community of organizations that establish the cloud-based environment. The organizer of the community is the authority of the systems used in the cloud. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

A public cloud environment is designed by a provider that wants to offer services to consumers (Figure 7.8). Based on the provisioning of the cloud environment, the cloud provider can offer access at a cost to consumers or as a service through other avenues, such as a search engine offering an analytics service to cloud consumers who want to leverage their offering. Google Cloud's search engine is an example of a public cloud. It is open access, but users can access additional features by signing in. The cloud provider that develops the public cloud environment is responsible for ongoing maintenance, operations, customer support, and availability. Depending on the offering, the provider will design and implement an architecture to support the consumer's needs.

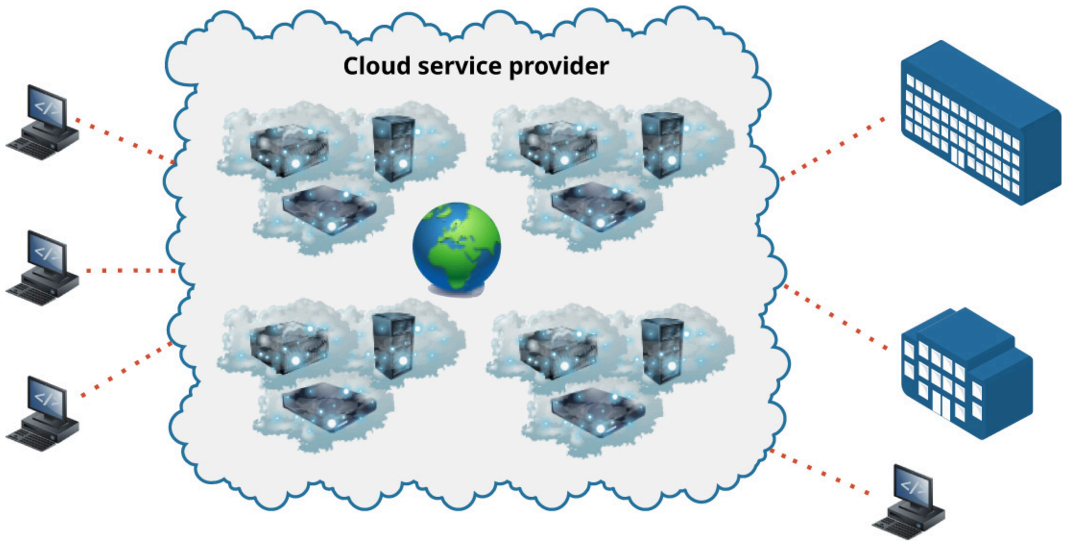


Figure 7.8 Cloud-based environments are available to individuals and business users and can be accessed in the public cloud. Access to the cloud-based environment is dependent on the policies that are imposed by individual providers. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

GLOBAL CONNECTIONS

Global Use of Search Engines

The public cloud provides access to information throughout the world. Each public cloud provider has domain locations that allow for global access. For example, Google hosts its own search engines in its cloud infrastructure. Because the company is based in the United States, the domain name for the Google search engine is google.com, but when users access Google in another country, the domain name has a country code appended to it. For example, in Mexico, the domain is google.com.mx. Using country-specific domains allows Google to tailor the search engine to adhere to laws and regulations in that country and to offer results in the country's language or languages, while ensuring all of their global users have access to a similar search engine.

A private cloud environment is designed by an organization based on its need for its own cloud environment (Figure 7.9). The private cloud provides access to resources that can be used and previsioned by the level, locations, and needs of the different parts of the organization. Whether its IS resources are internal or external, the management of the private cloud is the responsibility of the organization. What distinguishes this cloud environment is that the organization is both the provider and consumer of the environment.

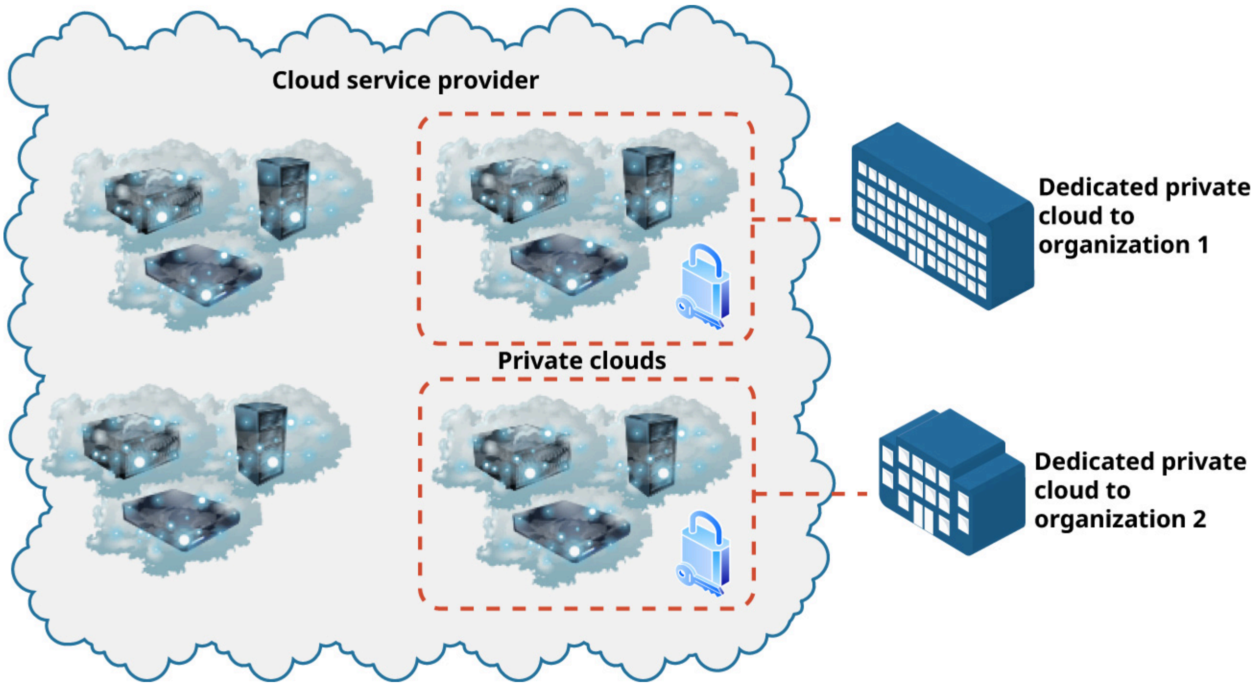


Figure 7.9 A private cloud-based environment incorporates a cloud-based database service. The purpose of the environment determines the configuration of the services and information technology resources that are built into the cloud-based environment. Private cloud environments are built to a specific cloud customer, and only that cloud customer has access to the environment. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Hybrid cloud environments are designed through the use of several deployment models (Figure 7.10). The most common hybrid cloud environment combines the deployment of a private cloud with controlled access with a public cloud without access requirements. This provides the organization with one environment for sensitive or confidential information and one for general use. The hybrid cloud can be a challenge to create because it requires the integration of two independent environments, which can be a website in the public cloud and a database service in the private cloud, that may be spread across different cloud providers.

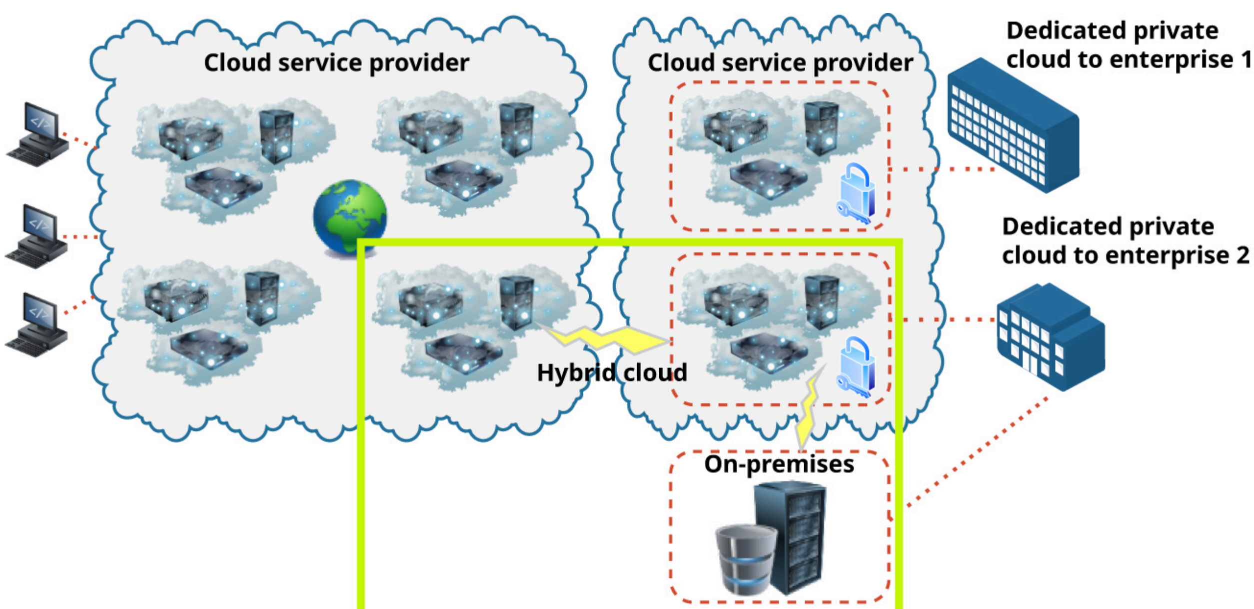


Figure 7.10 Depending on the requirements of the cloud consumer, the cloud-based environment can be a combination of private and public. The hybrid cloud can also combine an on-premise and cloud-based environment. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

When a cloud consumer is determining the value of employing a cloud environment, there are several factors they must consider, such as cost, services, and networking. The cost factors will require the involvement of senior management and finance because the organization will need to determine the different types of cloud environments, the different requirements of the environments, the level of support needed internally and externally, and the differences between the cloud provider's offerings.

An organization may choose a hybrid cloud environment so that it can control access to its information based on customer profiles. For example, if a retailer sells TVs, it might list models that are priced similarly to its competitors on its public website as part of the public portion of its hybrid cloud. The retailer might not advertise some other models that are at a special price that is only accessible to customers after they sign in to the private portion of the hybrid cloud. Similarly, a company may have a public site for direct sales to consumers, and a private site for retail merchants purchasing their goods wholesale.

LINK TO LEARNING

Hybrid cloud environments can be especially beneficial for organizations that have sensitive data and also want to increase sales to their customers. Read this article describing the ways banks can leverage AI and machine learning in a hybrid cloud (https://openstax.org/r/109AIHybridCld) to improve fraud detection and customer experience overall, while protecting their sensitive data and adhering to industry regulations.

Organizations will need to determine the need to move to a cloud-based environment or maintain an on-premise IT environment by conducting a feasibility study. This study should include but is not limited to considering up-front and ongoing costs as well as capital expenditures. An **up-front cost** is one that must be expended for services before delivery. Up-front costs are analyzed for both the on-premise and cloud environments, as they pertain to startup, hardware, integration, and implementation, among other expenses. An **ongoing cost** is one that must be expended for day-to-day operations. Ongoing costs are associated with software licensing, hardware maintenance, utilities, and labor. A **capital expenditure** is the cost for the acquisition of assets. Capital expenditures are those funds that are used to acquire value for the organization. Each organization sets the number of purchases to determine as such. Since each IT environment and cloud environment varies, the **total cost of ownership**, which is the investment in a product for the lifetime of the product, and the **return on investment (ROI)**, which is a metric that determines the value of an investment, will vary because of the differences in the cloud-based environment developed by the cloud consumer.

Major Cloud Service Providers and Their Delivery Models

The growth of cloud environments has been spurred by consumers wanting access to services that could provide more connections, such as a mobile app that searches the local eateries and then gives them access to the restaurant's menu. Organizations such as Amazon, Google, and Microsoft started small and have developed their own cloud-based environments that have changed the way organizations do business, moved the e-commerce space forward in time, and provided access to the world around us.

Amazon Web Services grew out of an internal need for Amazon to have the IT resources to manage and maintain its own IS environment. Amazon has taken its proprietary technology and grown the company into a cloud provider that offers services for other organizations to use so that they do not need to manage or maintain any on-premise systems. Amazon Web Services provides services such as computing, network service, databases, and storage; computing tools for organizations for analytics and machine learning; and services to help organizations with security, identity protection, and compliance.

Google evolved from a search engine to another cloud provider. Just like AWS, Google provides computing, storage, database, and networking services. Google Cloud provides its consumers with operations, development, and analytics tools. Google has also developed AI to simulate human intelligence and has created solutions using generative AI offerings. Google's offerings are built around its own cloud environment.

Just like AWS and Google, Microsoft Azure offers computing, databases, networking, and storage. Microsoft Azure made progress in the AI realm with services that combine it with other technology. Each offering by Microsoft Azure is built on Microsoft's foundation.

Amazon Web Services, Google, and Microsoft Azure all offer certifications in their respective platforms. Amazon Web Services offers multiple certification levels: foundation, professional, associate, and specialty. Each of the certificates is knowledge and role based, depending on the goal of the certification. Google offers foundational, associate, and professional certifications as well. Google structures its certifications around knowledge, fundamental skills, and technical skills. Microsoft also offers certification tracks in other areas of its products, such as AI, to support its cloud environment.

CAREERS IN IS

What Are Information Systems Certifications?

When looking at a career in IS, check out certification expectations with companies such as AWS and Google. These sites show some of the certifications that the industry often requires for a person to work in a cloud-based environment. There are certificates that are offered by the cloud-based providers, such as AWS and Google. There are also certifications that are designed around industry-based knowledge, like the Cloud+ certification offered by CompTIA. It is common for organizations in the industry to identify specific certifications in their job listings so that they can hire people who already have cloud, security, or project management certifications. Obtaining certifications appropriate for your preferred role before seeking employment can make you a more viable candidate for an open position.

The big cloud providers such as AWS, Google, and Microsoft offer a wide range of services to cloud consumers. However, there are smaller cloud providers that specialize in specific services. These smaller companies offer the cloud consumer an alternative to using mainstream providers. For example, DigitalOcean offers development environments that are focused on only development, and Wasabi only offers cloud-based storage. These specialized services provide more options to the cloud consumer, so they may need to do additional research to determine whether their needs are best met by a provider that can offer a variety of services or one that specializes in one service.

Organizations in today's business environment have to stay competitive in order to continue to grow and operate. This is sometimes identified as a competitive advantage, the factor that allows one company to make products or offer services more efficiently and effectively than its competitors. One advantage an organization might investigate is how it deploys IT resources over its competitors. Information technology resources are a cost factor that must be considered when determining the advantage one company might have over another.

An organization may choose to add to their competitive advantage by moving into a new area of its **market share**, which is the sales that a company has in its industry, usually calculated as a percentage. This move will require additional IT resources to support the initiative.

The organization can follow two courses of action to select their service provider: issue a **request for quote**, which is the process for determining the pricing of IT resources based on the organization's understanding of what is needed, or a **request for proposal**, which is documentation of the details of a project, including the IT resources that might be needed, in order to support the bidding process to get a fair and competitive price. Both processes will provide the organization with information about the possible up-front cost to start the project and the ongoing cost of maintenance for the IT resources.

The benefit of going through the bidding process is that it will help the organization identify the capital expenditures that are needed to accomplish the project. This step is needed to determine if sufficient funds are available. The next step, confirming the total cost of ownership of the IT resources, is needed to validate the availability of funds in the projected budgets for subsequent fiscal years. Once the total cost of ownership is determined, then the organization can evaluate the return on the investment of the IT resources that are purchased. The return on investment will influence the total cost of producing a product, entering a market, or introducing a new service.

7.3 Cloud Computing Technologies

Learning Objectives

By the end of this section, you will be able to:

- Identify the technology components in cloud computing
- Discuss migration strategies and best practices
- Identify cloud-based standards in industry

The technical components of cloud computing range from advances in networking to the possibilities of virtualization. For each aspect of cloud computing technology, there is a component that creates a feature, service, or tool that a consumer needs. These components interlock to build the foundation for cloud computing.

When organizations choose to migrate their systems, data, and services to the cloud, they should identify and follow best practices. Each organization will develop its own best practices based on trial and error, lessons learned, and the plans that other organizations have used. Each organization will build its migration strategies to accomplish its goal, which is to have a successful transformation to the cloud.

As part of any transition in service, an organization will need to verify the applicable industry standards and regulatory requirements and ensure they adhere to them. There may be international, federal, and state regulatory requirements they need to follow.

Technology Components in Cloud Computing

Since the development of the cloud environment, there has been specific network architecture needed, such as more availability to control the flow of data, how it manages access to the applications, and bandwidth capabilities. Traditional network architectures did not meet these requirements, which led to the development of SDNs. The SDNs changed the way networking components worked and handled traffic, and they opened new methods of controlling the network architecture. The SDNs move from the proprietary software and configurations of network equipment manufacturers to develop a mechanism to enable control at specific levels of the network architecture. The other aspect of SDNs is their ability to virtualize the network infrastructure, enabling the network manager to control the network infrastructure from the SDN controller (Figure 7.11). The SDN controller provides centralized management of the network environment, the application layer manages the applications and provides information to the SDN controller regarding the needs of the applications, and the infrastructure layer is the layer where the physical network hardware resides.

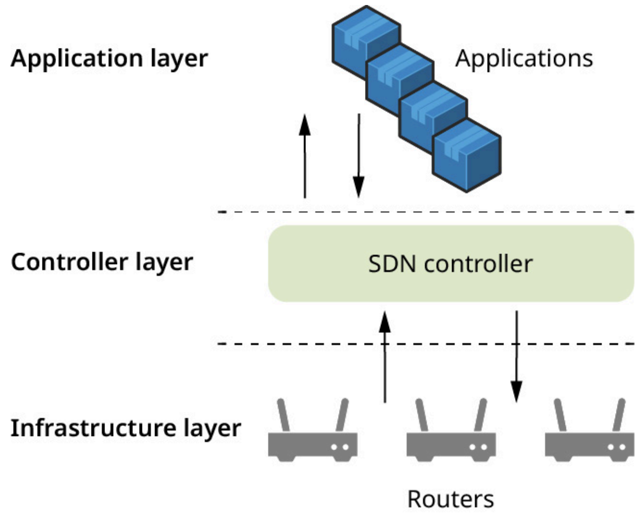


Figure 7.11 The components of a software-designed network (SDN) are broken into three layers: application, controller, and infrastructure. Each layer has its function within the SDN structure. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit "Routers": modification of work "Router (16624) - The Noun Project" by Christopher Pond/Wikimedia Commons, CC0 1.0)

Advances in virtualization have changed the realm of network storage. Virtualization has enabled network storage to be expanded, meaning that cloud consumers can access more storage. It has also offered more options for developing customized storage solutions for customers.

Today, there are cloud computing providers that specialize in storage only. They have taken the **storage-area network (SAN)**, which is a network that provides high-speed connectivity to a storage environment, and introduced virtualization to it and expanded the storage capabilities (Figure 7.12). Changing the traditional SAN into a virtualized environment creates a pool of virtual servers that can now be used as a cloud storage environment. This virtualization of SAN has also changed the requirement for a large amount of physical storage, thus changing the cost factor for both the cloud provider and the cloud consumer.

With every change comes challenges, such as the introduction of broadband networks, which provided cloud providers with needed bandwidth but also created greater security concerns. Increasing throughput and network capacity along with the increased bandwidth means an increase in the need for security tools for cloud providers and their consumers. The cloud consumer expects to be able to trust that the cloud provider has the necessary security tools in place to protect their data at the same time they provide availability to the data.

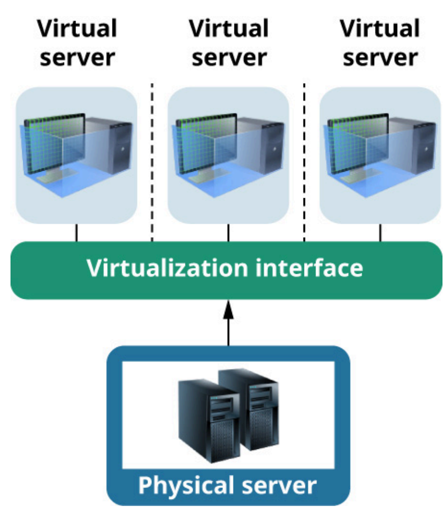


Figure 7.12 The first component to virtualize a server is a physical server. The next is a virtualization interface tool to inventory the resources of the physical server and allocate them into the virtual server environment. Once the tool is implemented, the virtual server environment can be built out. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

LINK TO LEARNING

The use of virtualization tools in the cloud environment is a necessity—especially in the area of server virtualization—as a way to increase the performance, availability, and reliability of a cloud service. Read this article about the specific placement of the virtual machine in the cloud system (https://openstax.org/r/109VirtMachPlc) to understand how researchers determined that placement can affect efficiency.

Migration Strategies and Best Practices

When an organization evaluates the possibility of migrating (moving) their systems, data, and infrastructure to a cloud-based environment, they must determine their **migration strategy**, which is the plan an organization will follow to move to the cloud. This migration must be laid out in a manner that upholds the organization's business strategies. Some best practices that an organization might consider for migration are the following:

1. Identify the goals and objectives of the organization. This process will help the organization better understand its need for a cloud-based environment and what advantage the environment will offer the organization.
2. Evaluate cloud providers to select the one that maximizes the business's strategies. The evaluation process is a step that will identify the advantages and disadvantages of each of the cloud providers considered for the transition to the cloud.
3. Design a plan for the migration. This process will require the involvement of the different departments in the organization. The final plan should be assessed to ensure it adheres to IT governance.
4. Implement a methodology for communication about the migration. This step is needed to create the procedures for communicating the progress of the migration to the different departments in the organization.
5. Develop a test plan for the migration, and conduct a practice run. The migration process should have a test environment in the plan to validate the **data migration tool**, which is a software-based tool that is designed to move data from one data repository to another, and the ability to migrate into the cloud-based environment. The practice run will prove or disprove the ability to migrate into the cloud.
6. Conduct the migration. During this step, the migration process moves forward, and the systems are moved to the cloud-based environment.
7. Employ a specialist for the migration on the new platform. This aspect of the migration may be covered by the cloud provider, or the organization migrating will have personnel to accomplish the process.

To select the migration tool to be used during the process, it is necessary to have chosen a cloud provider. Each cloud provider will have migration tools specific to their systems and specialists trained in them. Part of the practice run process will include testing the migration tools that the cloud provider uses, based on the amount of data to be transferred, the type of data to be transferred, and network constraints.

Another point in the migration plan is the funding of the project. This funding will require management support and the financial resources of the organization. In most migrations, the cloud provider offers an estimate for the cost of the process. This is only an estimate because there are variables that may change during the process. One such variable is the actual amount of data that are migrated because the volume will change between the time the migration plan is developed and when the process starts.

One process that an organization should require is compliance with the CIA triad (refer to Figure 5.2). Security in the migration process is a priority when selecting the cloud provider. There are many security standards that should be followed in the handling of data, such as the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard, which are discussed in Chapter 6 Enterprise Security, Data Privacy, and Risk Management. These security standards are dictated by international standards, federal regulations, and even state statutes. Security processes should then be laid out with the cloud provider to determine what type of identity and access management, network security, and data encryption the cloud consumer will require. This service will have to be accounted for in the estimate to fund the migration.

Cloud-Based Standards in Industry

When designing cloud-based solutions for an organization, the organization will need to research the cloud providers, the services available, the service levels required, contractual obligations, and even arbitration policies. After performing this due diligence, the organization will need to select and implement an international, federal, or state standard for the design process. One standard is the **NIST Cloud Computing Reference Architecture**, which is a federal standard that can provide direction for an organization in the selection process, industry definitions, and components of a cloud architecture. The NIST document will be informative and resourceful for an organization that is considering a cloud environment for the first time. Some cloud providers have frameworks in place to help organizations migrate into their cloud environment. The framework provides guidance, tools, and processes to migrate into the new platform, accounting for operations, performance, security, and cost.

When reviewing industry standards for cloud-based computing, organizations will need to continuously reference the different cloud service models, cloud deployment models, and cloud security standards that each provider offers. One such model is **Security as a Service (SECaaS)**, a cybersecurity service that a cloud provider offers to protect cloud consumers. It can be implemented across community, public, private, and hybrid cloud deployment models. Another model is **Firewall as a Service (FWaaS)**, which is a cybersecurity service that a cloud provider offers to protect the perimeter of a company's network.

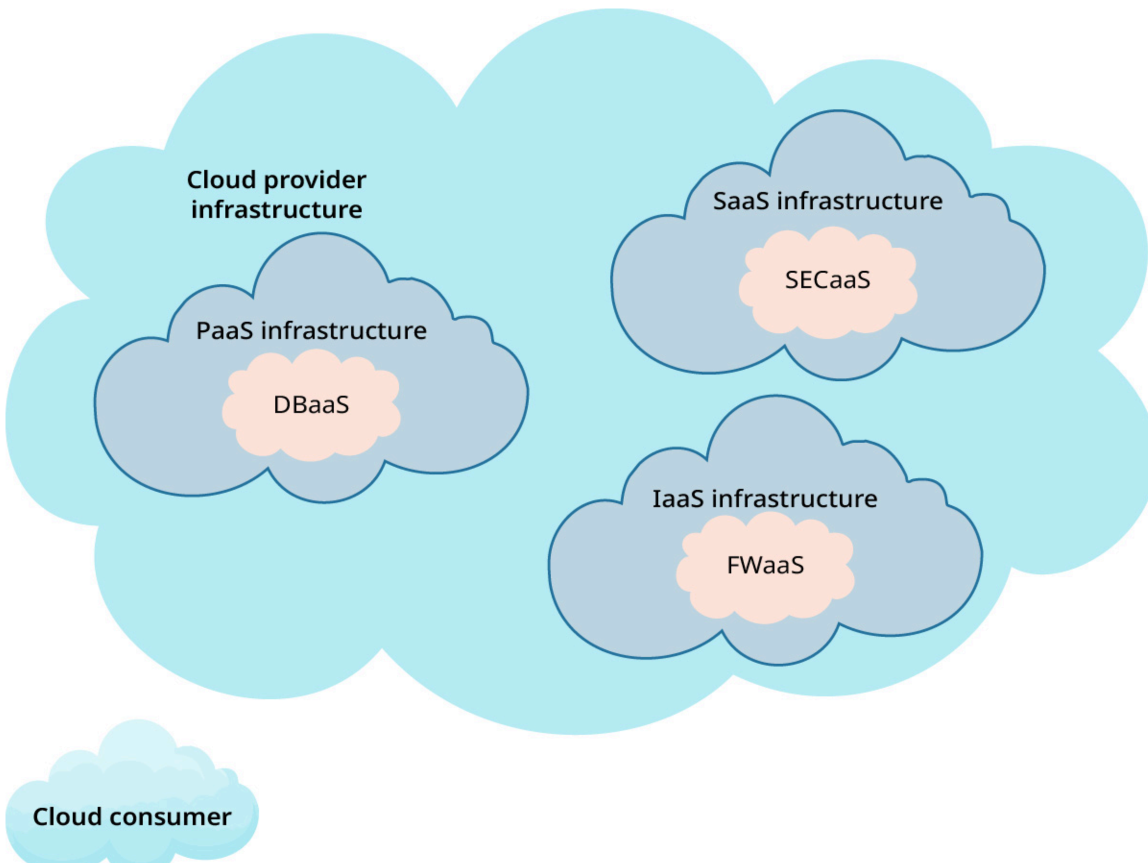


Figure 7.13 The three main parts of the cloud provider infrastructure are SaaS, PaaS, and IaaS. The SECaaS is a component of the SaaS infrastructure. The DBaaS is a component of the PaaS infrastructure. The FWaaS is a component of the IaaS infrastructure. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

One decision that an organization needs to make is the security standards to follow. The NIST Cybersecurity Framework, which, as you learned in 5.3 Information Security and Risk Management Strategies, is a federal standard that works in any computing environment. The framework provides guidance in the following areas (Figure 7.14):

- identifying, determining what in the organization needs to be protected;
- protecting, putting safeguards in place to build a structure for the protection of assets;
- detecting, implementing tools needed to identify cybersecurity threats;
- responding, implementing a strategy for the containment of any cybersecurity incidents; and
- recovering, restoring any system to operational status after a cybersecurity occurrence.

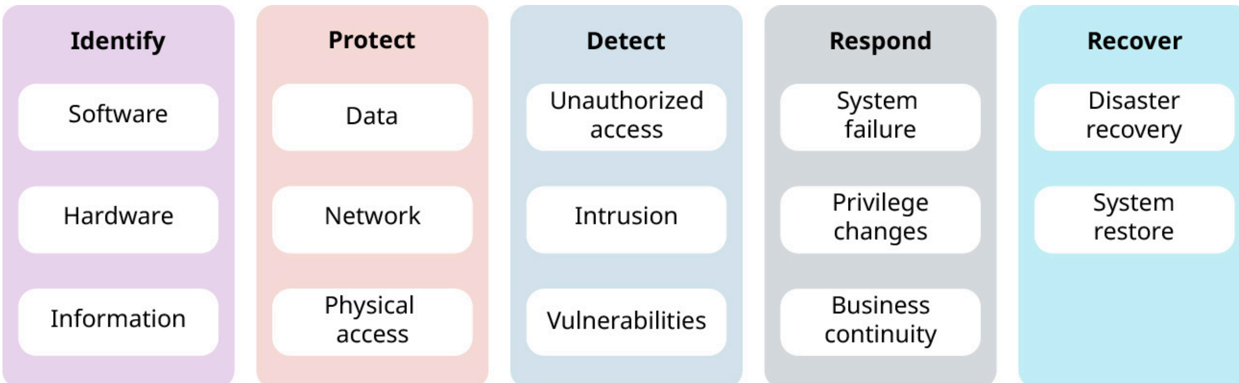


Figure 7.14 Each component of the NIST Cybersecurity Framework has a specific function in the cybersecurity framework. Organizations can create their own functions for each of the components. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The NIST Cybersecurity Framework provides a foundation for an organization to develop a cybersecurity program. It can be used in the development of policies for cybersecurity, risk management, business continuity, and disaster recovery plans.

FUTURE TECHNOLOGY

Cybersecurity Issues in Artificial Intelligence Use in Cloud Computing

Consider the future of cybersecurity as it pertains to cloud computing and then add a tool like AI. The use of AI in cybersecurity can greatly enhance the methodology used to identify potential threats to the cloud environment. The full extent of the opportunities that AI can add to the tools cybersecurity specialists use is unknown at this time, yet it can play a role in the defense of data. In fact, the Cybersecurity and Infrastructure Security Agency (CISA) has published its “Roadmap for Artificial Intelligence” to demonstrate how the U.S. cyber defense agency believes they can use AI responsibly to enhance and protect critical infrastructure.[4] The future of cybersecurity involves AI, so it is important to learn how to use it responsibly to protect and secure data. Reading about how CISA is using AI in cybersecurity can provide a foundation for this knowledge.

Case Study: Migrating to the Cloud

A company wants to restructure its IT resources and has determined that the cloud meets its requirements. It has compared the use of a cloud-based environment to the goals and objectives of the organization and concluded that the cloud-based environment will offer a competitive advantage in the organization’s industry. This restructuring will require the migration of the company’s systems to the cloud.

The organization will have project managers work with IT to develop a migration plan and submit it for approval for those specializing in IT governance. The plan will require that IT provide resources to configure

4 Cybersecurity and Infrastructure Security Agency, “Artificial Intelligence,” U.S. Department of Homeland Security, accessed January 20, 2025, https://www.cisa.gov/ai

the migration tool needed to move to this cloud provider's environment. The plan is laid out as follows:

1. Identify all assets to be migrated to the cloud.
2. Identify all licensing associated with the software currently used.
3. Meet with the cloud provider to determine which licensing will transfer or if licensing is provided in the contract.
4. Establish a test environment in the cloud.
5. Decide on the migration tool to be used and develop the migration application.
6. Test the migration tool in a practice run.
7. Review the information from the practice run to determine if the migration will be successful.
8. Establish a migration date and communicate it across the organization.
9. Conduct the migration.
10. Test and validate the migration.
11. Conduct a follow-up to the migration and create a lessons-learned document.

This is a simple outline of a process an organization might follow to migrate to the cloud. Each migration is different and has requirements that will vary depending on factors associated with the organization and the cloud provider.

7.4 Cloud-Based Industry Applications

Learning Objectives

By the end of this section, you will be able to:

- Identify the types and categories of applications in the cloud
- Determine when an enterprise application would be migrated to the cloud

Cloud-based applications can vary based on the industry and the needs of an organization. Examples of categories of applications include analytics, development, and e-commerce. One solution is a **commercial off-the-shelf** application, which is commercially produced software or hardware that is available for sale and is ready to install and use without customization. Another solution is a **home-grown application**, which is software that is developed for an organization in-house, based on the development requirements of the organization.

Types and Categories of Applications in the Cloud

Organizations are now challenged to look at their cost as it pertains to the different applications they use to operate in the market space. These applications carry maintenance and licensure costs. Each application will eventually need to be updated or replaced due to the software manufacturer's requirements. Replacement of the application is defined by the application itself and the number of seats allowed in the terms of the license.

Organizations are now turning to cloud-based applications to replace their current applications. These applications are hosted in the cloud versus a physical on-premise environment. The application is leased based on the same criteria, such as number of seats and volume of data, which are comparable to the purchase of the application. The difference is that instead of owning the application outright, the organization leases the privilege to use the application.

Companies like SAP, Oracle, and Workday offer cloud-based enterprise resource planning (ERP), which is a system that is used to manage the operations of an organization for customers that want to combine multiple organizational platforms into one. Figure 7.15 illustrates examples of platforms that can be combined into an ERP. The platforms are modular and can be configured to incorporate financial, supply chain, analytics, and other needs. The system gathers data and stores the data in a data warehouse where the data can be managed. The combination of systems can handle the analytics that organizations use in the decision-making process. Because the ERP system is customizable, the manufacturers build the systems according to each customer's requirements.

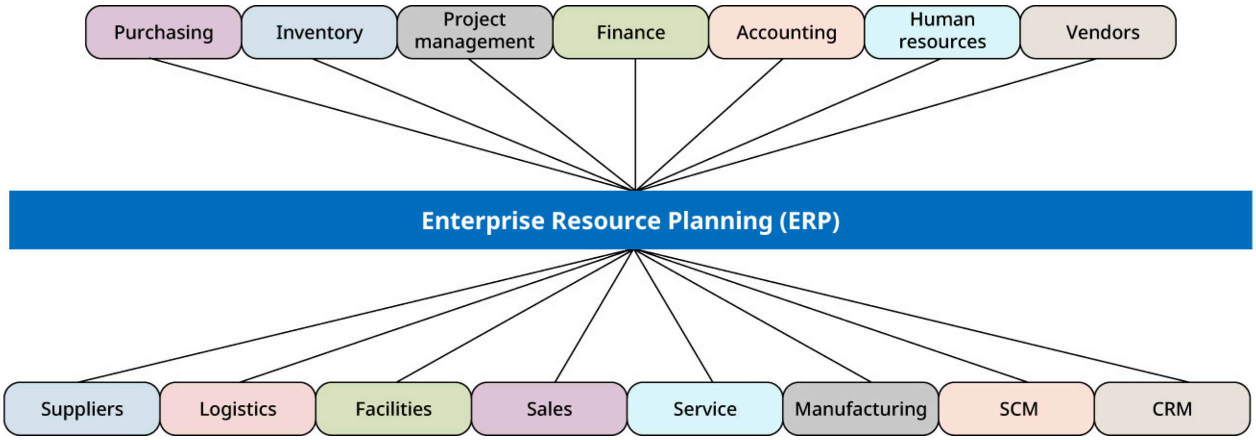


Figure 7.15 Enterprise resource planning (ERP) can include numerous possible components, as it is built to the customer's requirements. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Companies such as Salesforce, HubSpot, and Zoho have a cloud-based **customer relationship management (CRM)** application, which organizations can use to manage customer interactions and leads, and perform analytics. A CRM is used to determine the return on the organization's sales force investments in the customer base and uses a data warehouse for accumulating the data for analytics purposes. Figure 7.16 shows an example of a CRM. A CRM is a modular platform and is fully customizable based on the customer's requirements.

Figure 7.16 There are several possible components of a customer relationship management system (CRM). Each CRM is designed and implemented based on the customer requirements. The modules provide information for the system and the decision-making process. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Companies such as Infor, Oracle, and SAP offer cloud-based supply chain management systems. A **supply chain management (SCM)** system optimizes an organization's production and distribution of goods and services. The SCM has upper-level components, such as logistics, management, and profit. Like other solutions, these components are also customizable. For example, logistics will have functions such as managing inbound and outbound logistics. Each SCM is designed based on customer requirements and specifications. Figure 7.17 shows an example.

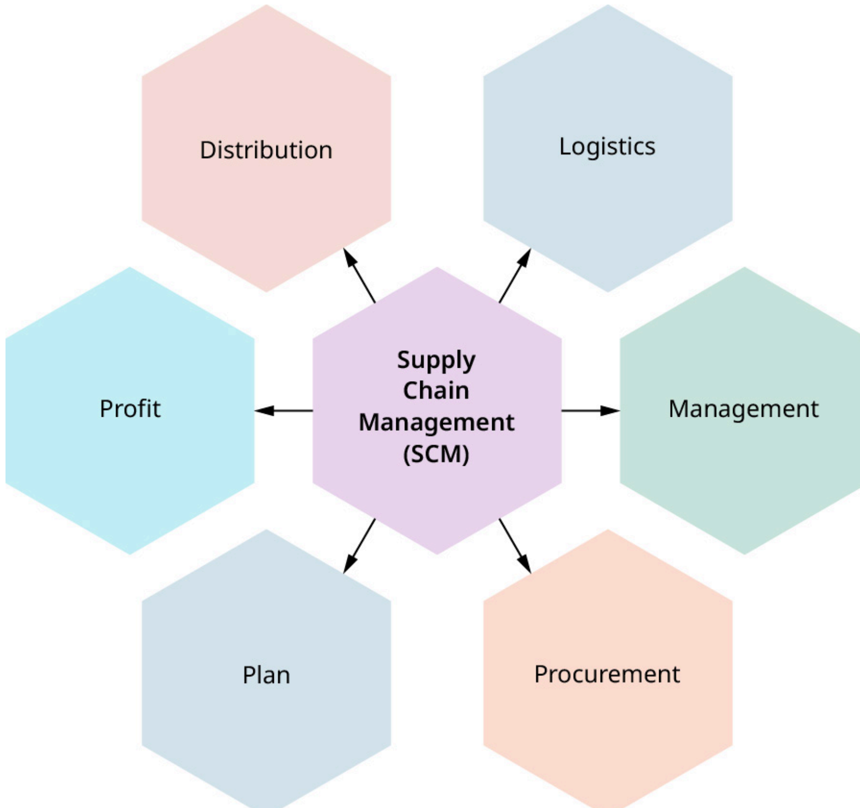


Figure 7.17 The primary levels of the CRM components are customizable to provide functionality, such as this example of a supply chain management system. The CRM system is fully customizable; therefore, other components are available. (credit: modification of work from *Introduction to Computer Science*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Companies such as Workday, BambooHR, and ADP offer cloud-based human resources (HR) systems. This type of system can be used for employee relations, performance evaluations, payroll, and benefits. This system operates a data warehouse that stores the data files for use in the analytics process. The components of the HR system are customizable, such as the application programming interface or the choice of the database system (such as Microsoft SQL or Oracle).

Each organization should evaluate their processes to determine which system meets the requirements of the operation. These requirements vary from organization to organization, which is the justification for the manufacturers constructing the systems in a modular layout. The organization will determine the functionality of the system by providing the manufacturer with details of its operation, and the outputs of each section of the organization, that need to be covered by the system.

The other aspect of these cloud-based systems is that one system covers all the functionalities of the others. The ERP system has modules for HR, CRM, and SCM built into its operational parameters.

Migrating an Enterprise Application to the Cloud

When an application, such as Microsoft Office 2016, is no longer supported, organizations will need to consider their next steps. These steps can be to replace the application with a different on-premise application or migrate their system to the cloud (Figure 7.18). Office 2016 could be replaced with Office 365, which acts like a cloud service with regular updates instead of an Office suite product that becomes obsolete. This decision has many factors, such as the difference in cost between the on-premise product and the cloud-based service. Other factors include licensing or system requirements. When the application is a **mission-critical platform**, which is an application or program that will cause a financial burden if there is a loss of service, then monitoring and management controls must be included in the migration process. A cloud computing platform provides technical support and security in moving applications to the cloud. Cloud computing services also offer the infrastructure, storage, and processing power to make a migration relatively easy.

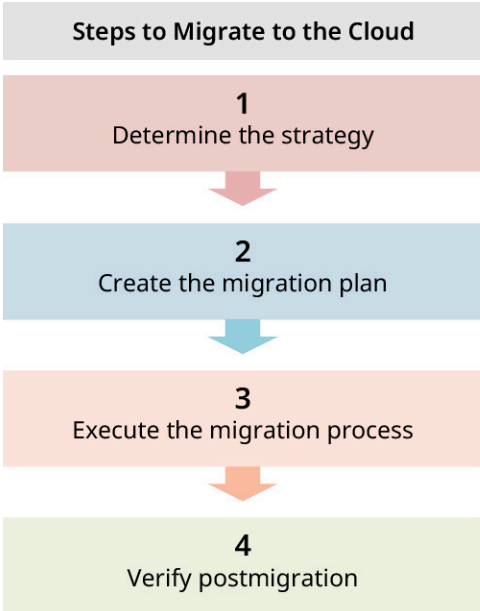


Figure 7.18 An organization may want to consider several steps before they migrate their data to the cloud. The migration process can be automated, yet the order, tools, and steps to be taken will need to be developed for the process. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

If an organization wants to use cloud-based application development, they must evaluate the tools that are available in the automation and optimization of the migration process. These tools can help reduce the cost of the migration process because of the reduced human interaction needed in the process. The automation process will aid in the data migration process, provided there is minimal configuration of the tools, since human interaction is required for configuration, which in turn drives the cost up. Each of the major cloud providers, such as AWS, Google, IBM, and Microsoft, have migration tools that are specialized for the cloud-based environment.

CAREERS IN IS

Automation in Data Migration

The use of automation tools in the migration of data requires personnel who are fluent in software development and proficient in programming languages. The job titles might be Cloud Automation Engineer or Senior Software Engineer. The person in this position will not only develop the tools, they will also need an understanding of the different environments the automation tool will be used in. This means that the professional in the position will need to be fluent in both the physical and virtual cloud-based environments.

GLOBAL CONNECTIONS

Software Development in Cloud Computing

Software development is not a local process anymore; it has moved to a global environment. Software development projects are not just handled by one group in an organization. Projects are shared across global organizations to expedite the turnaround and use personnel efficiently across the organization. Since projects are shared across the global development environment, there are requirements, laws, regulations, and standards that vary from country to country that have to be managed. This global connection allows for a project to have access to additional capabilities, but it also increases the complexity.

Case Study: Using the Cloud for Parallel Application Development

Organizations are often faced with the decision about whether or not to automate. When an organization's applications have reached the end of their life cycle, a decision must be made about what next steps should be taken. These decisions have both time constraints and funding needs associated with them. The organization will need to prepare for the development of the application, as features will have changed, processes may have changed, and the environment that IT operates in may have to change. This is the time in which the organization should have project management develop the process for the development of the application. Project management can help determine if the development of the application is considered a new project or is associated with change management. No matter which direction the organization goes with for the development of the application, the process will incorporate the software development life cycle (refer to Figure 4.7). The organization will need to prepare for the new application by starting with the software development life cycle (SDLC), which, as you have learned, is the process used for the development of software and applications (refer to 4.1 Systems Analysis and Design for Application Development). This process can include moving the application to a new computing environment, such as the cloud. Needing a new application is an opportune time to develop in the cloud. This is also the time to determine if the application will operate in a virtual environment.

The cloud environment offers an organization the opportunity to develop the new application in parallel with the old application, thus providing the organization with the ability to identify differences between the two. The parallel process offers the development team the chance to work with the end user to make a smooth transition. The parallel process allows for testing of features, especially those that might be new, and the ability for the end user to interact with the system and assist in verification of the processes.

7.5 Scientific, Industrial, and Social Implications of Cloud Computing

Learning Objectives

By the end of this section, you will be able to:

- Explain the scientific breakthroughs that made cloud computing possible
- Identify the social implications of cloud computing and its impact on data privacy
- Understand cloud-based sustainability

Cloud computing has made many advances since its inception. These advancements have been associated with the introduction of new technology, SDNs, and the growth of the internet. Each advancement has led to new opportunities in the cloud market space, which in turn has led to new offerings for cloud consumers and moving cloud-based computing into the mainstream of business today. Consider a scenario of vacation planning. In the past, people had to use travel agents to plan trips, but now there are many travel applications that allow a person to plan their own vacation.

With the move to the cloud, data privacy has become a relevant and timely topic. Another concern is the ethical use of data that reside in cloud environments. Further, consider the social impact of the amount of data stored in the cloud, which is accessible at any time of day by any device.

The sustainability of any market space is a question all organizations need to consider. In the market space of remote access, cloud-based computing is accessible to most people. It is available from any device without the addition of an application, software, or tool. This is a benefit that adds to the sustainability of the cloud.

Scientific Breakthroughs That Made Cloud Computing Possible

One of the most important breakthroughs in cloud computing was SDNs, which have changed the way network engineers manage traffic by offering scalability, which led to optimization of traffic performance through the infrastructure layer's ability to manage network resources, and the flexibility to design networking in a new manner using the functionality of the control layer. In the cloud computing environment, SDNs provide better management of network traffic, improve resource management, and give cloud providers tools to enhance their security profile. What makes the SDN platform so unique is that it is built on **open-source software**, free software that is available for use and modification without licensing, known as OpenFlow and OpenDaylight. There are also SDN platforms using Python-based language for programming.

Research continues today into possible alternatives to the current open-source software used. There may be alternatives because SDN architecture works with virtualization and bare metal platforms that are independent of the network equipment manufacturer. This independence offers more capabilities, flexibility, and security by not requiring a specific vendor for network equipment, which in turn allows for a layered approach to building out the cloud provider's network infrastructure. SDN architecture communicates across the three layers: application, control, and infrastructure (refer to Figure 7.11). The communication is facilitated by the API.

CAREERS IN IS

Software-Defined Network Cloud Architect

The state of network engineering has changed with the introduction of SDN. A position as an SDN Cloud Architect requires an undergraduate degree and may also require certifications in programming languages, cloud architecture, and virtualization. Changes in the network architecture require that the IT professional performing the duties is qualified and certified. These positions work with both physical and virtual environments, so the IT professional will need knowledge in physical equipment plus an understanding of virtualization software and systems.

Social Implications of Cloud Computing and Its Impact on Data Privacy

The social implications related to data privacy and security also connect to the ethical guidelines of an organization and the personal code of conduct of staff that access the data. In addition, it is important to consider the legal implications, jurisdiction issues, and operational requirements, plus national laws, state laws, and international standards, such as GDPR, System and Organization Controls, and California Consumer Privacy Act, that might control certain types of cloud service operations. Cloud computing systems use data marts, data warehouses, data lakes, and big data. A data mart is a data storage location that is a subset of a data warehouse. A data warehouse is a data storage location that accumulates data from multiple sources. A data lake is a repository used to store structured and unstructured data that are not size dependent. Big data is a large data set that is used for analysis. The storage of data by the cloud provider and the use of data by the cloud consumer must follow regulations and laws written for the protection and ethical use of the data. These regulations and laws are often specific to the industry, such as medical, financial, and educational areas.

Social implications that impact individuals in society involve use of the stored data. An organization's analysis of the data for decision-making can have positive or negative effects on society. Opening a manufacturing plant in an area that has a labor force can be considered a positive effect, whereas its impact on the natural resources of the area might be a negative effect. This is where the organization has to determine the impact their actions will have on society in that specific region.

The type of information that is to be produced from the data will dictate the type or tools that will be used to extract it. The data from the different storage platforms can be used to discover trends, make predictions for future growth in a product, and perform analytics to determine if the organization is growing as planned. The manner in which the data is to be interpreted also influences the type of tool used to extract it. There are tools that provide numerical information, visualization of the information, and general reporting. All of these factors are taken into consideration when selecting the right tool for the decision-making process.

ETHICS IN IS

Data Storage

The storage of data raises ethical concerns for organizations. Data privacy is always in the forefront when dealing with stored data because of the possibility of data breaches. The data that an organization stores are a target for potential hackers. It is required that organizations implement strong encryption practices, such as using algorithms like AES-256 and implementing end-to-end encryption for sensitive data, and access controls, such as employing multi factor authentication for log-ons and conducting regular security audits to identify vulnerabilities and ensure proper implementation of controls.

Information technology professionals must have a code of ethics when dealing with large amounts of data. This code of ethics is needed not only to protect the privacy of the data but to protect the integrity of the IT professional.

Cloud-Based Sustainability

In any industry, an organization must determine how to achieve sustainability in their products, services, and offerings. This issue is familiar to those who developed cloud computing. One factor that has led to the sustainability of cloud-based computing is its accessibility from any device. Creating a platform that does not require the adding of an app, software, or a proprietary component is a major factor in attracting and sustaining a strong customer base. It is also important to consider the environmental impact of cloud-based solutions, such as energy consumption of data centers, and reflect on how an organization can reduce its carbon footprint, such as learning what efforts are being made to recycle resources (for example, cooling water, using generated heat, and optimizing operations). These factors can help an organization determine what cloud-based solutions to use.

GLOBAL CONNECTIONS

Sustainability

Sustainability is a global commitment, whether it involves the environment or the continuation of a product line. Each cloud provider has different definitions for sustainability and different interpretations of the effects on the global market. An organization should review the cloud provider’s sustainability practices when evaluating the provider. As the cloud grows, the actions of the cloud providers improve sustainability in the form of growth and in the protection of the environment for the future. For example, Google promotes sustainability by pursuing net-zero emissions through technology and innovation, such as energy-efficient chips. Google Maps can provide traffic and emissions data that may help city planners make decisions about development and transportation systems, in turn, potentially supporting initiatives to make cities more environmentally friendly.

Another factor that can lead to sustainability is a provider's ability to offer services that can be created with automated tools by the customer, without needing to wait on hold for customer service, thus reducing the need for customer service interaction and, in turn, reducing the cost for assistance. The minimal time it takes for a cloud consumer to bring a system online, roll it into production, and start generating revenue is a major component of satisfaction and will lead to sustainability.

Each offering, each tool, each process, and each component that cloud-based computing puts in place benefits their sustainability. The potential for growth is sustainable, the possibility of continued offering is sustainable, and the new technology that emerges has the potential for sustainability.

Key Terms

bare metal server physical server that is deployed for a single business that provides the business full access to the server resources

business continuity plan that an organization puts in place to maintain its operational status in an emergency scenario

capital expenditure cost for the acquisition of assets

cloud computing (also, the cloud) information technology resources that are available through the internet on an on-demand or pay-as-you-go basis without the users needing to manage it

cloud consumer entity that uses and maintains access to computing resources of a cloud provider

cloud provider company that provides on-demand services such as data storage, applications, and infrastructure in a platform accessible through the internet

commercial off-the-shelf commercially produced software or hardware that is available for sale and ready to install and use without customization

Communication as a Service (CaaS) service that allows for the cloud-based delivery of services such as Voice over Internet Protocol, videoconferencing, and internet-based telecommunication services

community cloud infrastructure shared by multiple organizations with a common interest

customer relationship management (CRM) application that organizations use to manage customer interactions and lead management, and perform analytics

cybersecurity specialist person who identifies and develops security strategies, verifies needed security improvements, and implements security strategies for an organization

data migration tool software-based tool that is designed to move data from one data repository to another

Database as a Service (DBaaS) service that gives cloud consumers the ability to manage and maintain relational and nonrelational databases

delivery model resources offered by a cloud provider

deployment model location, method, and entity responsible for controlling the infrastructure

disaster recovery process an organization follows to reestablish operational status after an incident causes a system failure

elastic storage ability for a cloud storage resource to expand or collapse based on demand

end user entity that makes use of the technology provided by an organization

Firewall as a Service (FWaaS) cybersecurity service that a cloud provider offers to protect the perimeter of a company's network

home-grown application software that is developed for an organization in-house, based on the development requirements of the organization

hot site storage cloud service in which mission-critical data are stored in one location where the organization can have immediate access to the data

hybrid cloud combination of public and private models that can be combined with on-premise infrastructure

infrastructure facility and system used to support an organization's operations

Infrastructure as a Service (IaaS) cloud services deployment model that involves delivery of infrastructure resources, such as networking and storage

market share sales a company has in its industry, usually calculated as a percentage

migration strategy plan an organization will follow to move to the cloud

mission-critical platform an application or program that will cause a financial burden if there is a loss of service

network engineer person with the skill to design, implement, and manage a network in support of an organization's mission

network-attached storage (NAS) cloud service–provided storage system that is flexible and attaches to an organization's network infrastructure

NIST Cloud Computing Reference Architecture federal standard that can provide direction for an organization in the selection process, industry definitions, and components of a cloud architecture

on-premise environment physical hardware, such as servers, network equipment, workstations, and network infrastructure
ongoing cost expense for day-to-day operations
open-source software free software that is available for use and modification without licensing
Platform as a Service (PaaS) cloud services deployment model that involves management of the software and hardware resources for the purpose of development
private cloud infrastructure dedicated to a single organization
public cloud infrastructure that provides services in an on-demand environment
request for proposal documentation of the details of a project, including the information technology resources that might be needed, in order to support the bidding process to get a fair price
request for quote process for determining the pricing of information technology resources based on the organization's understanding of what is needed
return on investment (ROI) metric that determines the value of an investment
scalability ability of a resource to be scaled up or down with minimal effort
Security as a Service (SECaaS) cybersecurity service that a cloud provider offers to protect cloud consumers
service-level agreement (SLA) document that outlines levels of service that a cloud provider assures the cloud consumer they will receive
Software as a Service (SaaS) cloud services deployment model that involves delivery of applications in the cloud
software-defined network (SDN) network that uses software for traffic management in programmable controllers and interfaces
storage-area network (SAN) network that provides high-speed connectivity to a storage environment
supply chain management (SCM) optimization of an organization's production and distribution of goods and services
system administrator person who manages and maintains the information technology and information systems resources for an organization
Testing as a Service (TaaS) service that cloud providers have built to outsource testing of software, application, and other components that would normally be performed in the organization
total cost of ownership investment in a product for the lifetime of the product
up-front cost expense for services before delivery
virtualization service in which a physical computer environment creates a simulated computer environment

Summary

7.1 Fundamentals of Cloud Computing

- On-premise IS resources provide organizations with systems that are managed and maintained by the IS staff of the organization.
- Cloud computing has introduced a means by which organizations can provide services to their customers through the internet.
- Cloud computing provides constant access through the internet to any device from any location.
- Cloud computing maximizes resource use through the implementation of virtualization software, which adds scalability and elasticity for the cloud consumer.
- There are numerous IS positions available in cloud computing, such as network engineers, system administrators, and cybersecurity specialists.

7.2 Cloud Computing Services, Pricing, and Deployment Models

- Cloud computing incorporates a delivery model to allow consumers to build the cloud computing environment that will best handle their computing needs. Those delivery models are IaaS, PaaS, and SaaS.
- Cloud computing has a deployment model that enables the cloud consumer to build an environment

structure that meets business strategies. The deployment models are community, private, public, and hybrid.
- Cloud computing offers consumers flexibility, scalability, and pricing variations based on usage.
- The cost factor of cloud computing versus on-premise environments should be evaluated before organizations enter any contracts.
- Each cloud provider is different, and the services they offer differ based on their customer profiles.

7.3 Cloud Computing Technologies

- Technology used in cloud-based computing, such as SDNs, virtualization, and storage-area networks, provides some of the functionalities offered to cloud consumers.
- To properly migrate to cloud-based computing, organizations must determine what migration tools are needed to complete the move to the cloud infrastructure.
- Security of the data is essential when it comes to migrating to a cloud-based platform. Security frameworks such as NIST and the CIA triad will help with the process before, during, and after.
- Organizations need to identify a cybersecurity framework that maximizes the protection of their data.

7.4 Cloud-Based Industry Applications

- Organizations need a variety of cloud computing applications and must choose the category and type to be developed, purchased, or leased.
- Organizations will encounter software or applications that the vendor stops supporting and will need to determine whether to replace the software or migrate to the cloud.
- Organizations can research the possibility of migrating to a cloud-based application versus on-premise deployments.
- In a migration strategy, organizations can determine if the application migration can be automated to reduce costs.

7.5 Scientific, Industrial, and Social Implications of Cloud Computing

- The evolution of technologies and software has moved cloud-based computing into the mainstream of business.
- Ethics must drive an organization's use of data because of social implications and data privacy laws and regulations.
- Cloud-based computing will need to continue to look at new forms of revenue to accomplish sustainability.

Review Questions

1. What term describes a physical computing environment that is located at an organization's facility?
- **a.** on-premise
- **b.** hot facility
- **c.** cold site
- **d.** cloud-based

2. A cloud environment incorporates physical hardware to deliver services that are described in what way?
- **a.** programmable
- **b.** virtualized
- **c.** tested
- **d.** rack mounted

3. What is the term for the party that manages and maintains a cloud-based environment?
- **a.** service provider
- **b.** ISP engineer
- **c.** cloud provider
- **d.** cloud engineer

4. What factor offers the cloud environment flexibility, utilization of system resources, scalability, and a cost factor that is scalable?
   a. cloud computing
   b. physical environment
   c. coding
   d. virtualization

5. What is the term for a plan that an organization puts in place to maintain its operational status in an emergency scenario?
   a. business continuity
   b. recovery plan
   c. emergency recovery
   d. shutdown plan

6. What is the first level of the cloud environment that must be designed based on the requirements of the cloud consumer?
   a. Infrastructure as a Service
   b. Platform as a Service
   c. Software as a Service
   d. Database as a Service

7. What is the second level of the cloud environment that is to be built in relation to the Infrastructure as a Service component?
   a. Database as a Service
   b. Software as a Service
   c. Platform as a Service
   d. Communication as a Service

8. What service allows cloud consumers the ability to manage and maintain relational and nonrelational databases?
   a. Infrastructure as a Service
   b. Software as a Service
   c. Testing as a Service
   d. Database as a Service

9. What is the term for an environment that is owned by a specific community or cloud provider that is offering services to a specific community?
   a. hybrid cloud
   b. community cloud
   c. public cloud
   d. private cloud

10. What is the term for an environment designed to use several deployment models?
   a. community cloud
   b. public cloud
   c. private cloud
   d. hybrid cloud

11. What advancement changed the way networking components worked, handled traffic, and opened new methods of controlling the network architecture?
   a. SDN
   b. VPN
   c. ACD

d. ATM

12. Advances in what area have changed the realm of network storage?
    a. networking
    b. virtualization
    c. programming
    d. architecture

13. What would an organization use to move their content to a cloud provider?
    a. programming code
    b. command line
    c. migration tool
    d. solution plan

14. What type of legal document is the NIST Cloud Computing Reference Architecture?
    a. state law
    b. industry guideline
    c. commercial code
    d. federal standard

15. What is the name of the guidelines that provide a foundation for the organization to work from and develop a cybersecurity program?
    a. NIST Cybersecurity Framework
    b. NIST Cloud Computing Reference Architecture
    c. NIST Standard for Cybersecurity and Risk
    d. NIST Computing Security Standard

16. What is a component of an enterprise resource planning system?
    a. company goals and implementation plans
    b. customer relationship management
    c. mission-critical platform
    d. home-grown application

17. What is an example of a cloud-based application used by companies such as Salesforce, HubSpot, and Zoho for managing their customer interactions, lead management, and analytics?
    a. enterprise management planning
    b. customer relationship management
    c. supply chain management
    d. automatic call distribution

18. What is a component of a supply chain management system?
    a. payroll
    b. customer interactions
    c. employee evaluations
    d. logistics

19. What is the consideration for planning that involves needed resources, maintenance, licensing, and utility cost?
    a. funding amounts
    b. quotation numbers
    c. cost factors
    d. loan values

20. What can aid in the data migration process when there is minimal need for human interaction?

a. machine learning
b. customized configuration
c. programming language
d. automation process

21. What platform is unique in that it is built on open-source software known as OpenFlow and OpenDaylight?
    a. SDN
    b. ATM
    c. TCP/IP
    d. VPN

22. What factor related to an IS professional who accesses data relates to the ethical guidelines of the organization when discussing social implications, data privacy, and security?
    a. job description
    b. personal code of conduct
    c. job requirements
    d. manager's approval

23. Cloud computing systems utilize data marts, data warehouses, data lakes, and big data storage techniques for the accumulation of what?
    a. control system data
    b. database backups
    c. raw data
    d. management logs

24. What repository is used to store structured and unstructured data and is not size dependent?
    a. big data
    b. data mart
    c. data warehouse
    d. data lake

25. What component of cloud-based computing is influenced by its accessibility from any device?
    a. competitiveness
    b. drive
    c. profitability
    d. sustainability

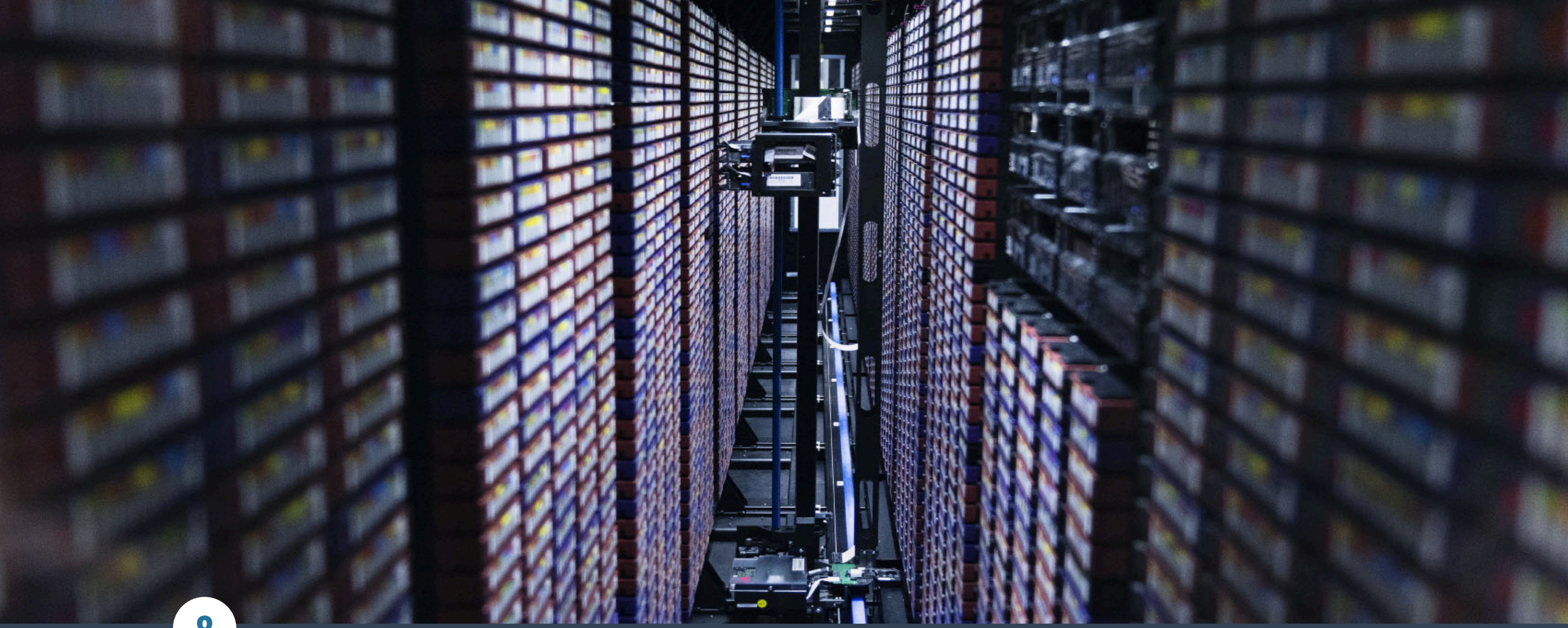
Check Your Understanding Questions

1. In your own words, describe what cloud computing offers the cloud consumer.
2. What does virtualization offer the cloud environment?
3. What are three examples of specialized careers for individuals who work in cloud computing?
4. What factors need to be covered when an organization adds new information technology resources to the cloud-based environment?
5. In your own words, describe Platform as a Service.
6. Identify and explain the purpose of each of the three primary delivery models offered in cloud-based computing.
7. Identify and describe the use of the four deployment models used in cloud-based computing.
8. What are two courses of action an organization can take when acquiring new cloud-based environments?

9. What are the primary delivery models for cloud-based computing?
10. In your own words, describe some advantages of using a software-defined network in a cloud-based environment.
11. What are the components of the CIA triad?
12. What are some additional cloud service models that are available?
13. What are the components of the NIST Cybersecurity Framework?
14. Each application has a life cycle in which it must be updated or replaced due to the software manufacturer's requirements. What is the term for this life cycle?
15. List four of the modules of an enterprise resource planning system.
16. List four modules of a customer relationship management system.
17. List four modules of a supply chain management system.
18. Describe the parts of a cost factor that might be used to determine if migrating to the cloud is cost effective.
19. How have software-defined networks (SDNs) changed the way network engineers manage traffic?
20. One factor that has led to the sustainability of cloud-based computing is accessibility. Describe accessibility as it pertains to cloud-based computing.
21. Identify the different types of storage that an organization has access to in a cloud-based environment.

Application Questions

1. Consider the skills needed to become a systems administrator in cloud computing. On top of the administration skills, what additional skills are needed?
2. When evaluating the possible uses of a hybrid cloud, identify one that a retail store might use.
3. What are the functions of the NIST Cybersecurity Framework and how are they applied?
4. If an organization's application is deemed to be at the end of its life, what two production environments can be considered for the new application?
5. What should an information technology professional develop to adhere to regulations and laws when handling data?



8 Data Analytics and Modeling

Figure 8.1 Data analytics can involve analyzing large volumes of data to help guide business decisions. (credit: modification of work “2022 Data Center” by Aileen Devlin, Jefferson Lab/Flickr, Public Domain)

Chapter Outline

Introduction

In today’s world, all types of businesses across every industry rely on data analytics to some degree. Companies now more than ever recognize the incredible potential behind this growing resource and use it to gain actionable insights, make informed decisions, and increase revenue. The purpose of data analytics is to extract meaningful information from huge amounts of raw data. This is how modern organizations differentiate themselves. At the heart of data analytics lies the foundational skills needed to reveal patterns and generate insight. For example, a company might want to know how well their product is performing in a specific market. By delving into the data, they may uncover trends such as higher sales during certain seasons, preferences for specific product variations, or correlations between marketing campaigns and sales spikes. These patterns offer valuable insights into consumer behavior and market dynamics, enabling the company to optimize its marketing strategies, tailor products to meet customer needs more effectively, and ultimately enhance overall performance in target markets. In the realm of business operations, the application of data analytics provides a foundation for informing the business analysis process and empowers organizations to make informed decisions based on insightful interpretations of market trends and consumer behavior. The goal is to produce results that generate insights that help management team members make decisions that have the greatest impact on an organization’s success.

8.1 The Business Analytics Process

Learning Objectives

By the end of this section, you will be able to:

- Define the terms associated with data analytics
- Identify the importance and challenges of collecting and using big data
- Describe the process of data acquisition
- Explain the business analytics process

The process of **data analytics** involves examining datasets to draw conclusions and insights, typically using statistical and computational methods to inform decision-making or solve problems. It involves techniques and processes for exploring data, often with the aid of technology, to drive actionable intelligence. Analytics is a tool that enables organizations to derive competitive advantage by analyzing historical data, forecasting trends, and optimizing business processes.

The evolution of analytics is described as having three distinct eras:[1]

- Analytics 1.0: focused on data warehouses and traditional business intelligence (historical reporting and descriptive analytics)
- Analytics 2.0: the rise of big data with unstructured and high-velocity data, driven by new technologies like Apache Hadoop
- Analytics 3.0: a modern era where businesses blend big data with traditional analytics to create data products that deliver real-time value

Big data allows organizations to gain a comprehensive understanding of their target market and customer base. For example, have you had the experience of searching for a particular item online, such as a new pair of shoes, and then noticed that your social media feed is inundated with ads for shoes and related items? This is a result of the kind of automated market research resulting from data analytics. Organizations gather information about features such as customer demographics, preferences, purchase history, and online behavior. Using this information, analysts can identify patterns and trends. Then, leaders on the marketing team can tailor the organization's products, services, and marketing campaigns to meet the specific demands of their customers, enhancing customer satisfaction and loyalty.

Importance of and Challenges with Big Data

Every generation presents a new disruptive technology that changes the face of business for those who recognize the potential. Innovations such as the cotton gin, textile mills, the steam engine, and the telegraph all revolutionized some aspects of the world and pushed technology along. In the future, historians will add to this list the processing of big data, which is an extremely large set of structured and unstructured data that cannot be processed or analyzed using traditional database and software techniques. British mathematician Clive Humby is credited with stating, "Big Data is the new oil."[2] If he is right, then analysts and companies that recognize the potential for insight will be those who "strike oil" in the business world. So in a sense, like oil extraction, the modern breakthrough is **data mining**, or analyzing large datasets to discover patterns, trends, and insights using statistical and computational techniques. Companies like Google have led the way with marketing tools that capitalize on big data, helping organizations better understand consumer behavior.[3]

1 Thomas H. Davenport, "Analytics 3.0," *Harvard Business Review* 91, no. 12 (December 2013): 64–72, https://hbr.org/2013/12/analytics-30
2 Clive Humby, "Data Is the New Oil," lecture at Association of National Advertisers conference, Orlando, FL, April 30–May 2, 2006.
3 Christena Garduno, "How Big Data Is Helping Advertisers Solve Problems," *Forbes*, March 15, 2022, https://www.forbes.com/sites/forbesagencycouncil/2022/03/15/how-big-data-is-helping-advertisers-solve-problems/

Challenge: Volume

The collection and use of big data have become increasingly important in today's business landscape, yet harnessing the very real potential of big data comes with significant challenges. The sheer volume, velocity of production, and variety of data can overwhelm those who cling to traditional data management and analysis methods. Analysts report that by 2025 the global volume of digital information is expected to reach 200 zettabytes.[4] Organizations must grapple with storing and processing enormous amounts of data. Designers and analysts need to work together to create and maintain scalable infrastructure capable of hosting advanced analytics tools.

Challenge: Quality

In addition to volume, the quality of big data poses challenges, as unstructured and noisy data can hinder accurate analysis and interpretation. This has prompted concern in situations where data analytics is key to success. Reliability issues stem from multiple causes. They can include inaccurate data, redundant entries, and simple human error in data entry.

Duplicated, or redundant, entries are multiple entries placed in the same dataset by mistake. There are various methods to respond to redundant entries. The first and most obvious is to simply remove them. Data engineers may use tools such as basic Python code and spreadsheet functions to filter out corrupt data at prescribed levels to produce a more accurate dataset. Input tools such as QR code scanners can help by automating the process. Another technique to address the issue of redundancy is to assign another value to an **outlier** (an observation that deviates significantly from the rest of the dataset), potentially indicating anomalies, errors, or unique patterns that require special attention during analysis. In other words, you would choose a value with significantly lower impact on the dataset to replace the outliers, such as an average value.

Challenge: Governance

Have you ever had your identity stolen? If not, you may know someone who has. These concerns relate to privacy and data governance, which is the overall management of the availability, usability, integrity, and security of data used in an enterprise. At the business level, companies do their best to comply with regulations and protect sensitive information. However, enforcement of strict digital privacy laws can vary from state to state, or nation to nation. Companies that do business in Europe must also abide by Europe's General Data Protection Regulation (GDPR), which as you may recall from 6.1 Key Concepts in Data Privacy and Data Security, is a leading global regulation in terms of enforcing transparency in how data are handled and strictly forbids the purchase and sale of personally identifiable data while allowing individuals the right to be forgotten. The GDPR is built upon several fundamental principles aimed at protecting the personal data of individuals within the European Union (EU). Refer to 6.4 Managing Enterprise Risk and Compliance to review these fundamental principles.

Challenge: Actionable Insights

The process of systematically using statistical and logical techniques to review, sort, and condense data for the purpose of gaining insight on areas of interest is called **data analysis**. Effective data analysis is critical for ensuring that the information is accurate so that an organization can then extract actionable insights from it. Extracting these insights is, however, a significant challenge. First, it requires special training to increase skills and expertise in this area. Data scientists and analysts must possess a combination of statistical knowledge, programming skills, and domain expertise to navigate the complexities of big data analysis. Additionally, it is important to be able to comprehend the results and to communicate them effectively to a broad audience. Incorrectly linking correlation to causation during data analysis can be an issue with both experts and software, and false positives and false negatives can lead conclusions astray. Additional challenges can arise from the regulations in some regions, such as the EU, that prohibit collecting and storing meaningful data to

4 Steve Morgan, "The World Will Store 200 Zettabytes of Data by 2025," *Cybersecurity Magazine*, February 1, 2024, https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/

ensure privacy or decrypting encrypted data.

LINK TO LEARNING

Explore the transformative power of big data in the article "Big Data: 6 Real-Life Business Cases," which delves into six compelling real-world examples (https://openstax.org/r/109BigData) where big data analytics have revolutionized business operations across diverse industries.

Data Acquisition

With modern web analytics tools, companies analyze market trends and competitor activities in real time. By collecting and analyzing data from various sources—including social media, industry reports, customer reviews, and online forums—organizations can stay well-informed about market dynamics, emerging trends, and competitor strategies. Interested key decision-makers can then use this information to identify opportunities, anticipate market shifts, and proactively adapt their business strategies to maintain a competitive edge.

Analysts employ several methods to identify and acquire data from various sources, such as web scraping, sensor data collection, social media monitoring, data marketplaces and application programming interfaces (APIs), and internal data collection. Moreover, social media monitoring offers a window into public sentiment and trends, while internal data sources provide valuable organizational insights. These methodologies form the cornerstone of modern data analysis practices.

Automated extraction of data from online sources, typically using software to simulate human browsing behavior and retrieve information from web pages, is called **web scraping**. These techniques involve employing automated tools or scripts that can gather relevant information from multiple web pages, including but not limited to customer reviews, social media data, news articles, or publicly available datasets.

With the proliferation of Internet of Things devices, analysts can use **sensor data collection**, which involves gathering data from sensors designed to detect and respond to physical or environmental conditions, such as temperature, pressure, or motion. These sensors generate real-time data on parameters like temperature, humidity, location, or movement, providing valuable insights for industries such as manufacturing, health care, or logistics.

Social media monitoring involves monitoring and collecting data from social media platforms to gain insight into customer sentiment, behavior, and trends. By analyzing social media conversations, comments, likes, and shares, analysts can identify emerging topics, consumer preferences, or even potential brand issues.

Some organizations provide data marketplaces or application programming interfaces. A **data marketplace** is an online platform or ecosystem where data providers and consumers can buy, sell, or exchange datasets and related services. These marketplaces facilitate the discovery, transaction, and access to data in various formats, often integrating tools for analytics, visualization, and compliance management. An **application programming interface (API)** is the means by which software applications communicate and interact with each other for the purpose of exchanging data and functionality. These platforms offer a range of data sources, including financial data, weather data, demographic data, and industry-specific datasets. For example, a search using the Google search engine can also lead to ads on Facebook based on user data. Additionally, when you engage a search for specific items, such as a new smartwatch, your query becomes a data point that may be gathered and shared with companies tagging the term "smartwatch." This will prompt marketing tools in sites like Facebook and Instagram to promote customized ads with smartwatches.

The final main methodology for data acquisition is collection from internal data sources. Organizations often have extensive internal data sources, including transaction records, customer databases, sales data, or operational logs. Analysts can tap into these sources to gather relevant data for analysis and gain insight into their own business operations. This can represent a challenge gathering accurate data if the source becomes adversely affected, such as when a natural disaster occurs.

When collecting big data, analysts should also adhere to ethical considerations, follow data privacy regulations, and obtain proper permissions or consent when required. The importance of big data collection and use cannot be overstated. Organizations that can harness the power of big data gain a competitive edge by leveraging valuable insights for strategic decision-making. However, the challenges associated with big data, including its volume, quality, and the need for specialized skills, must be addressed effectively to unlock its full potential. By overcoming these challenges, businesses can capitalize on the immense value that big data offers and pave the way for innovation, growth, and success in the data-driven era.

The Business Analytics Process

The business analytics process consists of several stages, each one often influencing and informing the next. The process enables organizations to derive actionable insights from data (Figure 8.2).

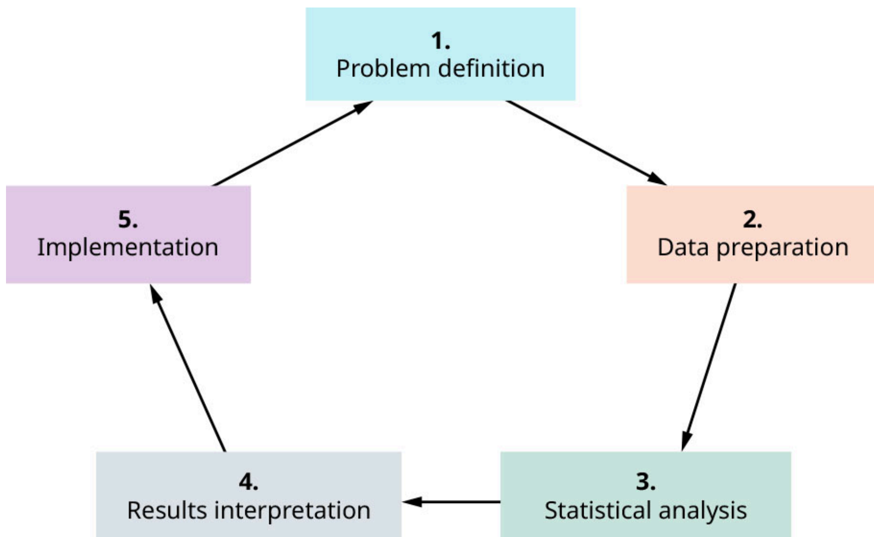


Figure 8.2 The business analytics process begins with problem definition, paving the way for data preparation, analysis, interpretation, and implementation. Note that in some cases, it may be necessary to repeat as new problems may have been identified in the process. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Step 1: Problem Definition

The first step in the process is problem definition. Here, the company sets out to name the problem or challenge that needs a solution that involves using analytics. To illustrate this process, consider an organization studying botany that sets out to classify varieties of iris. By clearly defining the problem, organizational leaders can focus their data analytics efforts and ensure alignment with the organization's goals. They can then begin to gather information to form the classifications.

Step 2: Data Preparation

Next comes collecting, cleaning, and transforming the data for analysis. This step includes gathering data from various sources, integrating separate datasets, and ensuring data quality. That can be a cumbersome task, since the organization will attempt to address issues such as missing values, outliers, or inconsistencies. Techniques for data cleaning and data transformation, such as data normalization or feature engineering, may be applied to ensure the data are suitable for analysis.

Data normalization involves adjusting data so that they have a standard scale, making it easier to compare different types of values. It ensures that one feature does not dominate others due to its scale. Dividing irises into categories is a relatively simple analysis and does not require data normalization. Other examples that would benefit from data normalization include comparing salary in thousands of dollars to years of experience, or comparing house prices and sizes. In the latter example, normalizing the size (by dividing all sizes by the largest size) can put that variable on a comparable scale to prices.

Feature engineering is transforming raw data into useful inputs for a model by creating, modifying, or selecting features (data points). It helps models understand patterns better by making relevant information more accessible. As an example, for predicting house prices, creating a new feature like "price per square foot" combines raw price and size into something more insightful.

As a simple use case, imagine predicting student test scores using hours studied and study material pages read. These features can be normalized so that the number of pages read does not overpower the number of hours studied, and a feature like efficiency (pages read per hour) can be engineered to capture how productive a student is. Effective data preparation is crucial for accurate and reliable results in subsequent stages of the analytics process.

Data Acquisition

There are typically three methods of data acquisition: using built-in libraries, using external datasets, or manually entering data. Each approach has its own merits. Libraries can save time but may be incomplete if the data focus on some items that evolve over time, such as technology. External data are convenient, but large datasets may be challenging to work with, especially if there are multiple sources of data. Manually entering data could prove cumbersome, especially if time is an important factor.

Built-in Libraries

Many programming languages, like Python, can use built-in libraries for the purpose of testing models. If you use Python for data analytics, you'll find it equipped with powerful libraries of built-in code segments and datasets tailored for various tasks, such as NumPy and Pandas. NumPy is useful for numerical calculations, while Pandas excels in handling data analytics tasks.

With these available libraries, Python becomes an ideal choice for scientific analysis and data-driven applications. Let's use the classic public domain dataset for iris classification from R. A. Fisher[5] for this example. The following snippet shows the code for importing the library and creating a pie chart. The example output is shown in Figure 8.3. Note that the line from sklearn import datasets instructs Python to use the library sklearn, which allows access to data on the iris species. You are also importing the matplotlib to create the pie chart.

```
# Iris Species Data Study
# Import libraries
from sklearn import datasets
import pandas as pd
import matplotlib.pyplot as plt

# Load the Iris dataset
iris_data = datasets.load_iris()

# Create a DataFrame using the data and feature names
iris = pd.DataFrame(iris_data.data, columns=iris_data.feature_names)

# Add the species column by mapping the target integer values to species names
iris['species'] = iris_data.target_names[iris_data.target]
```

5 R. A. Fisher, "The Use of Multiple Measurements in Taxonomic Problems," *Annals of Eugenics* 7, no. 2 (September 1936): 179–88. https://doi.org/10.1111/j.1469-1809.1936.tb02137.x

```
# Plot a pie chart showing the distribution of species in the dataset
species_count = iris['species'].value_counts() # Count occurrences of each species
plt.figure(figsize=(7, 7))
plt.pie(species_count, labels=species_count.index, autopct='%1.1f%%', startangle=90)
plt.title('Distribution of Iris Species')
plt.show()
```

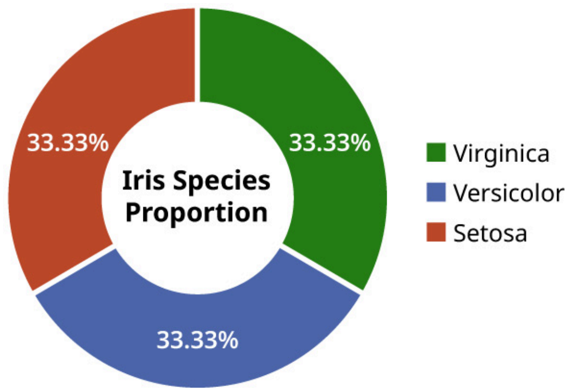


Figure 8.3 Python code was written to load and create a pie chart of various species of iris plants. (data source: R. A. Fisher, "The Use of Multiple Measurements in Taxonomic Problems," *Annals of Eugenics* 7, no. 2 (September 1936): 179–88. https://doi.org/10.1111/j.1469-1809.1936.tb02137.x; attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

You can observe how the code created a simple pie chart output to show the proportion of species of irises.

External Datasets

Using external datasets is the most common method of data collection. Here, the goal is to specify a path and a file name and then import the dataset from another location, which is often a spreadsheet or other standard data file type. The following Python code snippet accomplishes the same task as the previous example. The only difference is that it pulls the data from an external file instead of calling on Python's self-contained libraries.

```
# Pull Data from an Excel Spreadsheet
import pandas as pd
import matplotlib.pyplot as plt

# Load the Excel file
df = pd.read_excel('C:/Users/daxbr/iris.xlsx')

# Count the occurrences of each species
x = df['Species'].value_counts()
# Get the labels (species names) from the value counts theLabels
= x.index.tolist()

# Plot the pie chart of species distribution
plt.pie(x, labels=theLabels, autopct='%1.1f%%', startangle=90)
plt.title('Distribution of Iris Species')
plt.show()
```

In this example, Python is instructed to access an Excel file and run analysis on the information contained in the file.

Manually Entered Data

With a small enough dataset, a third option is to manually enter the information. The drawbacks of manually entering data include the time involved in entering data for a large dataset and the possibility of introducing errors in the form of typos. The following code snippet produces an output similar to the previous two examples:

```
# Enter Your Own Data
theSlices = [33.3, 33.3, 33.3]
theLabels = ["Virginica", "Versicolor", "Setosa"]
theColors = ['#96f97b','#ff81c0','r']

# Plot the pie chart
import matplotlib.pyplot as plt

plt.pie(theSlices, labels=theLabels, colors=theColors, autopct='%1.1f%%',
startangle=90)
plt.title('Iris Species Distribution')
plt.show()
```

The choice to use internal libraries, external data, or manually entered data is made on a case-by-case basis. In practice, it is important to keep in mind that data acquisition may involve a combination of methods depending on where the source data are for a project. For example, in this process where the hypothetical organization conducts a botany study, it may be most appropriate to use the built-in library, since features of iris plants have not changed recently and are generally agreed on in the scientific community. Manually entering the data would be unnecessary.

Step 3: Statistical Analysis

Once the data are prepared, data analysts apply statistical analysis to uncover patterns, relationships, and insights. This stage involves using statistical methods, machine learning algorithms, or data mining techniques, or a combination of methods, to explore and analyze the data (Figure 8.4). Depending on the nature of the data, analysts may employ descriptive statistics, regression analysis, clustering, classification, or predictive modeling. Analysts use these tools to run simulations. This provides opportunities to observe potential costs, predict return on investment (ROI), and identify metrics. Descriptive statistics help to give a "snapshot" of data and provide a jumping-off point for analysis.

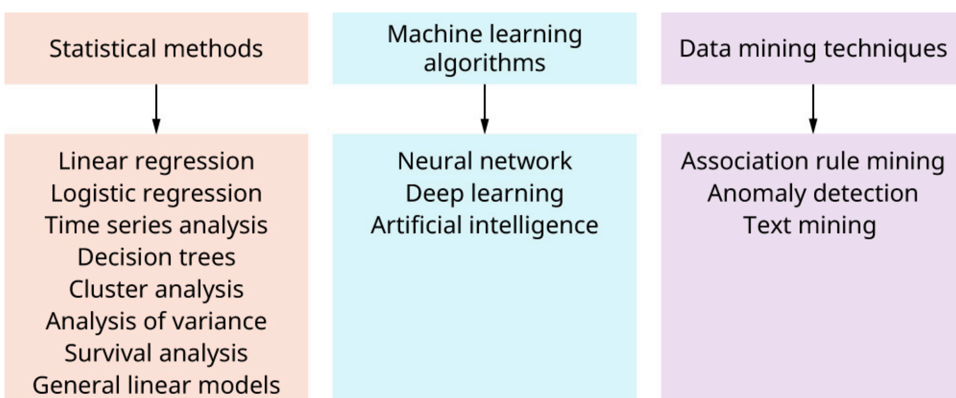


Figure 8.4 Some analysis methods can be categorized as statistical methods, machine learning algorithms, or data mining techniques, but many can fit into more than one category. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Causality or Correlation?

Correlation does not imply causation, but does one attribute affect another? Returning to the iris data, the following simple command can explore the correlation of sepal length and petal length (Figure 8.5).:

```
df.corr()
```

	SepalLength	SepalWidth	PetalLength	PetalWidth
SepalLength	1.000000	-0.117570	0.871754	0.817941
SepalWidth	-0.117570	1.000000	-0.428440	-0.366126
PetalLength	0.871754	-0.428440	1.000000	0.962865
PetalWidth	0.817941	-0.366126	0.962865	1.000000

Figure 8.5 The simple Python command generates a comparison of the lengths and widths of petals and sepals and shows a positive correlation between the sepal length and petal length. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

We can recognize that the petal length and the sepal length are strongly correlated; however, that correlation does not prove causality. It is a common pitfall for an analyst to believe that they have proven causation because of a strong correlation. The challenge in statistics is to remain objective and be cautious about using the word "proof." For example, there is 100 percent correlation between eating chocolate and being born. Every person who eats chocolate has been born, but being born does not cause one to eat chocolate. In the iris case study, we showed correlation between sepal length and petal length only. There is no evidence from this data that either sepal length causes petal length or petal length causes sepal length.

Step 4: Results Interpretation

The next step is results interpretation, where the insights are translated into actionable information. Analysts evaluate the findings in the context of the problem at hand, interpret the statistical results, and draw conclusions. They often create visualizations, charts, or reports from the data to effectively communicate insights to stakeholders.

LINK TO LEARNING

GeeksforGeeks has done their own analysis of the iris dataset (https://openstax.org/r/109IrisDataset) where you can notice a number of different visualizations of the data and the Python code that produced the output.

Step 5: Implementation

The best data in the world are functionally useless without action. In the final phase, implementation involves applying the obtained insights and recommendations to practice. This may involve strategic decision-making, process improvements, or operational changes based on the findings. Implementation may also require collaboration across departments or the integration of analytical models into existing systems or workflows.

LINK TO LEARNING

Exploratory data analysis (EDA) is the process of examining and understanding data to uncover patterns, trends, and relationships before formal modeling or hypothesis testing. Watch this video demonstration on

EDA using Python (https://openstax.org/r/109EDA) and the freely available iris dataset.

8.2 Foundations of Business Intelligence and Analytics

Learning Objectives

By the end of this section, you will be able to:

- Discuss the importance of business intelligence and analytics
- Explain how organizations use business intelligence and analytics
- Describe tools used in business and data analytics
- Evaluate various analytical models

In modern business management, organizations are constantly evaluating ways to leverage information and gain valuable insights to drive the decision-making processes. One way businesses can do this is by using predictive analytics, which can help identify emerging trends and consumer preferences, guiding product development efforts. For example, Netflix uses data to predict consumer preferences, which helps it determine which new series and movies to develop. Analyzing customer feedback and behavior can also help companies identify the most desirable features and incorporate them into their products. For example, Stitch Fix uses consumer preference data to design its own private-label fashion products, aligning them with popular trends.

Predictive analytics can also help businesses stay ahead of market changes by identifying emerging trends and opportunities. For example, L'Oréal Paris analyzed data from Google searches and social media to create a new ombre hair coloring kit, which allowed them to capitalize on a trend. Personalized recommendations based on consumer behavior can increase sales and customer satisfaction. For example, Amazon uses predictive analytics to preemptively ship products to distribution centers near consumers, reducing delivery time and encouraging purchases. Similarly, identifying regional patterns of demand and stocking preferences can help businesses reduce overstock and avoid stock-outs. For example, Walmart leveraged business intelligence tools to optimize inventory management and improve supply chain efficiency. They analyzed real-time sales data across stores using business intelligence (BI) dashboards and streamlined inventory costs and improved customer satisfaction by ensuring the availability of high-demand products. Walmart's BI-enabled decisions exemplify how actionable insights from data can drive operational efficiency and enhance customer experience.

The Importance of Business Intelligence and Analytics

You may have heard the phrase, "work smarter, not harder." This adage holds true for any industry. The success or failure of a business can come down to the ability to ask the right questions and thus make decisions that best capitalize on the finite resources available. The process of **business intelligence (BI)** involves collecting, analyzing, and interpreting data to inform business decision-making and improve organizational performance. Business intelligence seeks to provide a set of tools that allows decision-makers to do just that—work smarter instead of harder. Business intelligence tools offer numerous benefits to organizations across various business sectors. With BI, organizations can identify trends, patterns, and correlations within their data that could enable them to understand customer behavior, market dynamics, and operational performance. There are many additional benefits to using BI tools to enhance organizational management.

Valuable Insights

If data truly make up the "new oil," then that analogy can go a step further. Raw data—like crude oil—are completely useless until trained individuals use the proper tools to refine them. Once they refine the data, then business leaders can glean valuable information from that data. Simply put, the data are initially too overwhelming for humans to manually sift through. Data analytics automates the sifting process by deploying various analytics tools and algorithms to identify and highlight important information.

In the current business landscape, decision-making must be based on accurate and currently relevant information. Business intelligence and analytics play a vital role in this process. By consolidating data from various sources and transforming that data into meaningful insights, BI equips decision-makers with a comprehensive understanding of the organization's current state and its prospects. With analytics, decision-makers can evaluate different scenarios, perform predictive modeling, and simulate potential outcomes. These capabilities enable them to make informed decisions with less uncertainty.

Visualization

Another benefit of BI tools is the ability to produce a **visualization**, or a graphical representation of data and information to facilitate understanding, analysis, and communication of insights and trends. Many executive leaders may have a firm grasp on fundamental statistics, but they may lack the training and experience to derive real meaning from large amounts of data. This is where visuals are helpful for communicating vital information. Figure 8.6 shows a dashboard that is an example of an effective way to provide visual expressions from multiple data sources at once. A dashboard can facilitate easier communication of sometimes complex ideas more effectively, especially to an audience with minimal experience in technical fields.

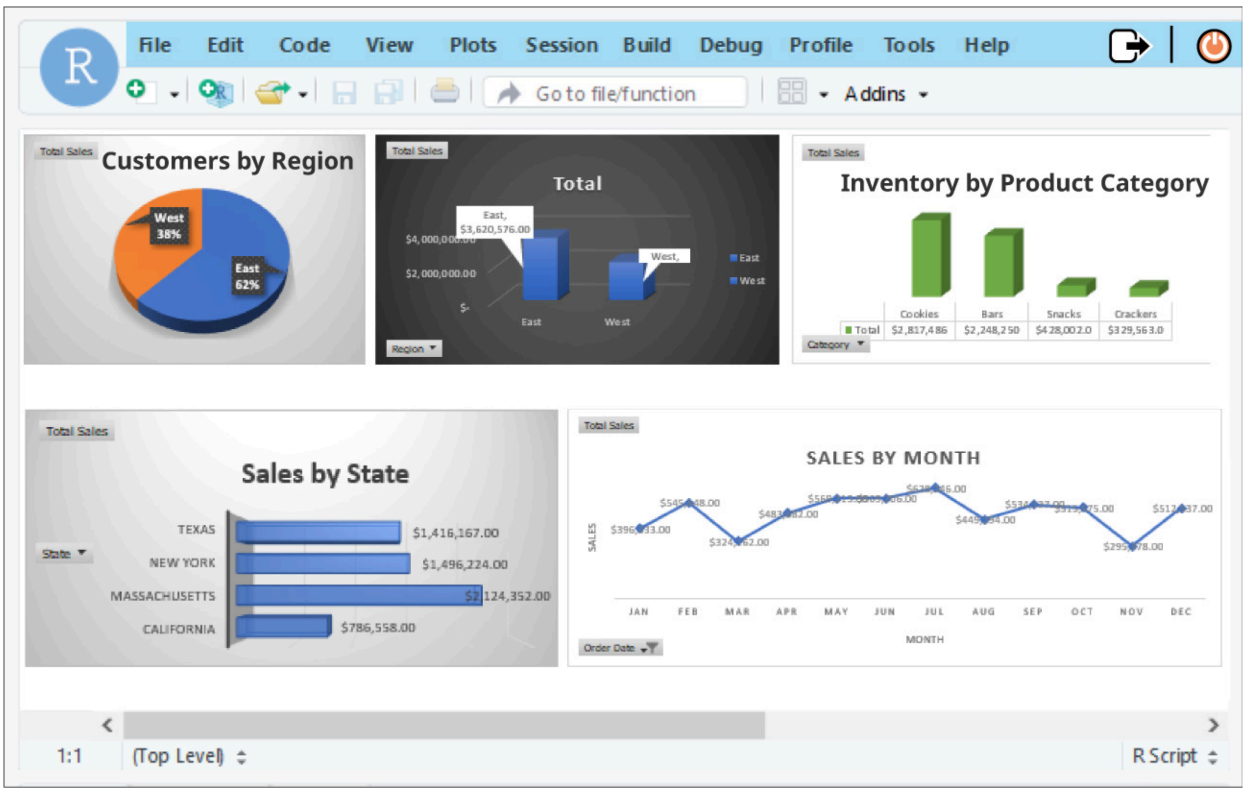


Figure 8.6 A dashboard tool brings metrics from multiple sources into one page for quick comparison. (credit: modification of work "Data visualization" by "Kabuttey"/Wikimedia Commons, CC BY 4.0)

Key Performance Indicators and Benchmarking

Business leaders are often analyzing how an organization is doing, and key performance indicators (KPIs) are an important part of that analysis. A **key performance indicators (KPIs)** is a measurable value that demonstrates how effectively a company is achieving its key business objectives and goals. Related to that is the concept of **benchmarking**, which is the comparison of an organization's performance against industry standards and competing businesses to identify areas for improvement and drive performance optimization. Business intelligence tools make it possible to identify KPIs and benchmark levels centered around efficiency, profit, and other metrics and assess the performance of the project or initiatives in real time.

Inventory Management

Business intelligence tools make life easier in terms of purchasing, procurement, and inventory management. Companies can generate reports on shipping and receiving and automate the process of ordering materials before they are below a certain threshold. Business intelligence also tracks outbound materials, so organizations can identify purchasing trends and reduce or eliminate wasteful spending. One way to quickly observe trends, costs, and other metrics is through a visual tool similar to the dashboard shown in Figure 8.6 that would instead show multiple metrics such as the on-hand quantity of products, the value of goods issued, and links to tasks such as ordering new stock.

Customer Analytics

The process of customer analytics represents a step forward in creating value from data by analyzing and synthesizing information about the customer, providing a customer-centric focus, and providing decision-making support. Through the careful analysis of customer data, business leaders can better understand the expectations, habits, and preferences of potential customers. These data are used to build consumer engagement and loyalty, improve the performance of marketing campaigns, and even identify additional distribution channels. It is helpful if customer analytics provides predictive recommendations.

For example, suppose you run a clothing store, and you wish to track the popularity of a specific design of pants. After you run some data queries on social media, mobile, and cloud media communications using web crawlers, you might discover a group of people with similar traits or features, as they are referred to in analytics. The results reveal that the typical customer is between twenty and twenty-four years old, and that the pants sell online 80 percent of the time (rather than in a physical store). This information indicates where your marketing efforts should be focused. In this case, the company should promote the pants online with less emphasis on the physical location and should direct ads to consumers under the age of thirty. To make that determination, an organization can use BI tools to conduct a **recency, frequency, and monetary (RFM)** analysis, which is the task of customer segmentation or grouping based on their purchasing habits. Essentially, four pieces of information are needed to create RFM scores:

- identity: depersonalized information, such as a customer ID
- recency: how long ago the last purchase was made
- frequency: how many purchases or conversions the customer made over a specified period
- monetary: total spent

Note that RFM is not strictly a tool used by for-profit companies. It can be beneficial for a variety of organizations, including hospitals and places of higher education. In health-care settings, RFM analysis can help prioritize patients based on their recency of visits, frequency of appointments, and monetary value of services utilized, facilitating targeted outreach and resource allocation. An RFM analysis can help with patient retention by classifying patients based on recent visits and service usage to design personalized follow-ups or wellness programs, and it can help with service optimization by prioritizing high-value patients for loyalty programs or preventive care services. In the education sector, RFM can help with targeted student engagement by identifying students who are most engaged (high frequency and recency of interaction) to tailor resources or interventions, and in donor analysis by recognizing high-value alumni donors based on donation patterns for optimized fundraising efforts. Using this information, you would then define an RFM score on a scale of 1 to 6 for each customer. An RFM analysis primarily focuses on behavioral data rather than personal traits like age or income level. While RFM analysis does not directly incorporate personal traits, it can indirectly reflect certain characteristics of customers based on their purchasing behavior.

Business Intelligence Tools Offer Competitive Advantage

In an environment where companies scramble to outdo one another, BI tools offer a competitive advantage crucial for sustainable success and also provide a pathway toward achieving this advantage. For people working in an increasingly competitive market, the ability to make fast decisions is part of the job, but knowing those decisions are based on hard evidence provided by data-driven insights offers greater confidence. By harnessing the power of big data, businesses can uncover hidden opportunities, identify emerging trends, and anticipate market shifts. This enables them to stay ahead of their competitors, respond quickly to changing customer needs, and capitalize on new business prospects.

By recognizing the benefits of BI and analytics, understanding the part these tools can play in decision-making, and leveraging them to gain a competitive advantage, organizations can position themselves for success in today's data-centric commerce environment. By deploying BI analytics tools, organizations gain superior insights into their operations, customers, and competitive landscape; find new potential customers; and make more well-informed decisions.

Customer data analytics can revolutionize business performance and customer loyalty. Data-driven customer insights are invaluable, but successful deployment requires a strategic focus on ROI and customer-centric innovation. Data are no longer limited to reporting; data are now deeply embedded in operational and decision-making systems. For example, companies such as Amazon, Google, and Netflix use data as a product to drive innovations like recommendation engines. Personalized offers and experiences make customers feel valued, increasing their loyalty to the company. Analytics is not just a tool; it is a strategy that aligns with a company's objectives and operations.

How Organizations Use Business Intelligence and Analytics

Organizations use BI and analytics across various functions of the business. Specific BI and analytics tools businesses can use to guide their operations include decision-making, time-series analysis, decision trees, marketing, financial analysis, and supply chain analysis.

Decision-Making

Business intelligence and analytics provide organizations with the necessary insights to make informed and strategic choices. By analyzing data from multiple sources, organizations can identify trends, patterns, and correlations that impact their operations. These insights enable decision-makers to evaluate different scenarios, assess risks, and determine the most effective course of action. For instance, a retail company analyzing customer purchasing patterns through BI might discover that certain products experience increased demand during specific seasons, prompting them to adjust inventory levels and tailor promotional strategies accordingly, resulting in optimized sales performance and customer satisfaction.

Time-Series Analysis

Time-series data consists of information collected on the same topic over a specified period. Examples can include the employment rate in a country over one year, the stock price of a specific company over the last year, or the attrition rate at a college from the fall through the following summer. Any data recorded continuously at different time intervals is considered time-series data. For example, Figure 8.7 shows a chart of time-series data from the National Park Service that compares horse population growth and foal production over several decades.

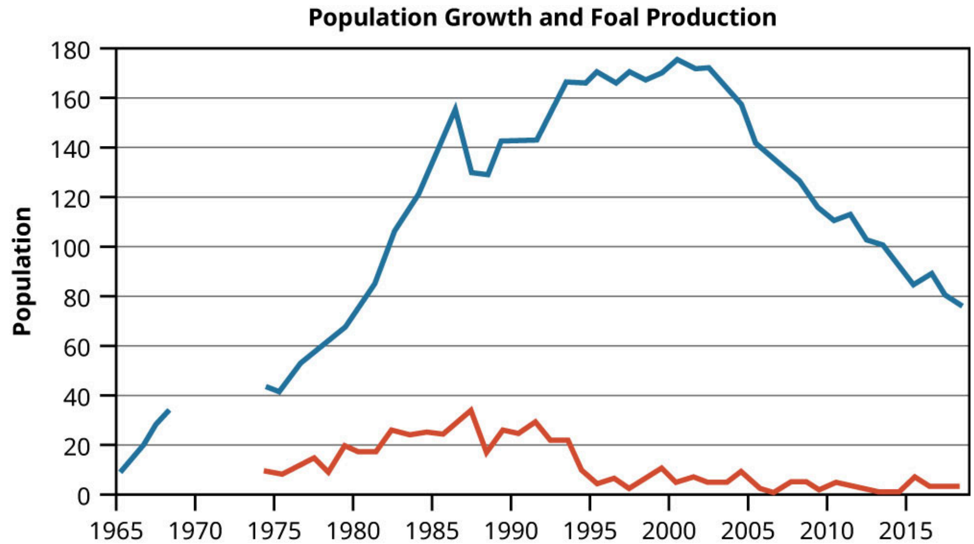


Figure 8.7 A time-series graph can compare multiple sets of data over the same period, such as the horse population growth and foal production on Assateague Island National Seashore, Maryland. The blue line represents the horse population, and the red line represents foal births. (credit: modification of work "Population Growth and Foal Production" by NPS/National Park Service, Public Domain)

Continuous time-series data refers to a stream of information that is collected or recorded over time without interruptions. It's essentially taking measurements or observations regularly, such as every minute, hour, or day, to track how something changes over a period. It could be, for example, monitoring temperature every hour throughout the day to observe how it fluctuates.

Decision Trees

Contemporary management challenges are not influenced by isolated decisions but rather by a series of decisions. Business leaders recognize the importance of how decisions made today may have a profound impact on future conditions. One analytics tool that speaks to this concept involves the use of decision trees. A **decision tree** in BI or data analytics is a decision-making tool that uses a tree structure diagram in which branches represent choices and their outcomes. They start with a question, then branch out based on the answers to subsequent questions, finally leading to a decision or prediction. For instance, in retail, a decision tree might help decide which customers are likely to buy a product based on factors like their age, purchase history, and location, helping businesses target their marketing efforts effectively.

Decision trees provide a framework to visualize the potential cause-and-effect relationship between decisions and future outcomes. They present a visual guide to show decision-making processes and future outcomes. The parts of a decision tree include the following:

- root node: the beginning, where the decision tree starts
- leaf node: the end, or the final output node
- splitting: dividing from decision nodes into subnodes according to the given conditions
- subtree: a subsection or branch

To better appreciate decision trees, consider Figure 8.8, which shows how it is possible to break down the decision of what drink to buy from a coffee shop. The first root node involves deciding between tea and coffee. If the customer decides to buy tea, they want it to be herbal. If the coffee shop does not have herbal tea, they want it to be iced. What if the coffee shop doesn't carry tea at all? What beverage will they drink then?

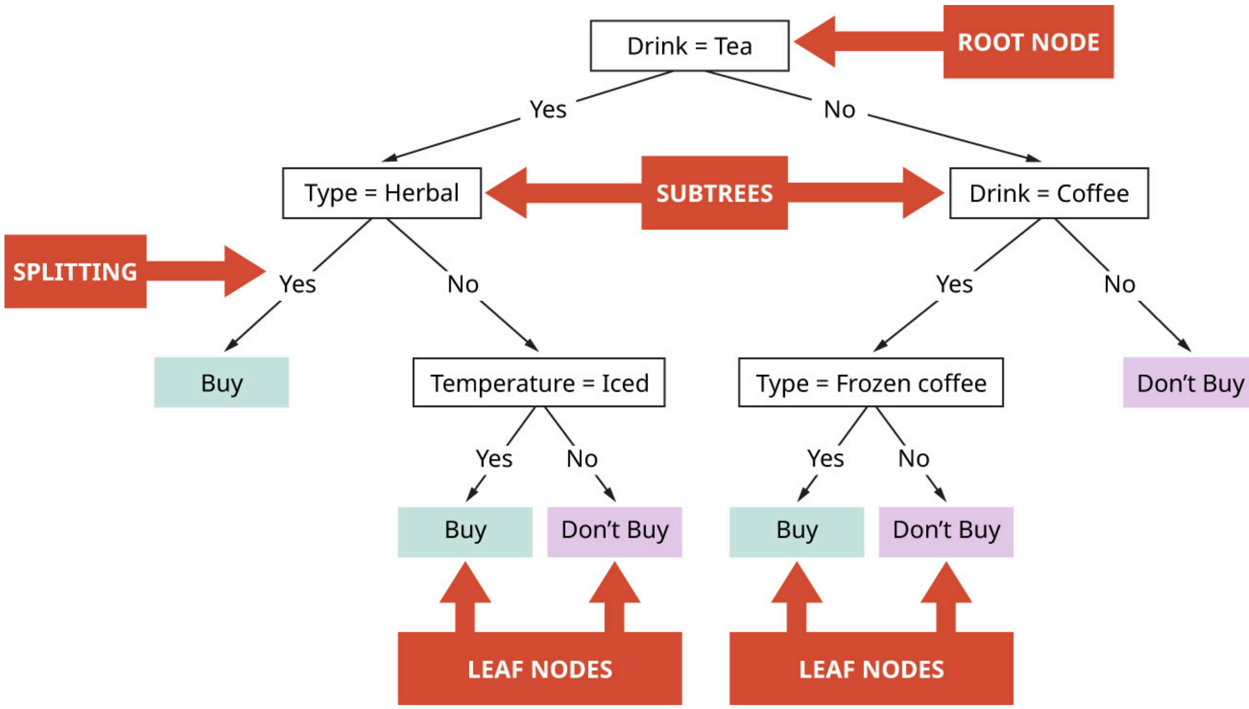


Figure 8.8 A decision tree can step through a user's choices for deciding on a drink at a coffee shop. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Marketing

Business intelligence and analytics also play a critical role in understanding customer behavior, preferences, and market trends. By analyzing customer data, organizations can develop targeted marketing campaigns, personalized promotions, and tailored product offerings. Targeted marketing involves knowing who your audience is and providing services accordingly. For example, Rakuten Travel understands that international customers prefer a clean, simple user interface, whereas potential customers from their home country of Japan typically prefer a busier page with more options, and Rakuten directs users to the appropriate version of the site accordingly.[6] Additionally, BI and analytics help organizations assess the effectiveness of marketing initiatives, track campaign performance, and measure customer satisfaction, enabling them to optimize their marketing strategies for maximum impact. In today's digital age, organizations leverage advanced BI and analytics technologies to assess the effectiveness of their marketing initiatives, track campaign performance, and measure customer satisfaction in ways that were not possible a decade or so ago.

For assessing the effectiveness of marketing initiatives, modern organizations harness the power of predictive analytics, machine learning algorithms, and data visualization tools.

When it comes to tracking campaign performance, real-time analytics platforms and marketing automation software play a crucial role. These tools provide organizations with immediate feedback on KPIs such as click-through rates, conversion rates, and engagement metrics. By monitoring these metrics in real time, organizations can make timely adjustments to their campaigns to optimize performance and maximize impact.

Furthermore, measuring customer satisfaction has been revolutionized by the advent of sentiment analysis tools and customer feedback platforms. These technologies allow organizations to analyze customer feedback from various channels, including social media, surveys, and online reviews. By understanding customer sentiment and identifying areas for improvement, organizations can enhance the overall customer experience and strengthen customer loyalty.

6 "Marketing Case Study #5: Rakuten Travel and the Target Market Strategy," Krows Digital, 2023, https://krows-digital.com/marketing-case-study-5-rakuten-travel-target-market-strategy/

In essence, the integration of modern BI and analytics technologies enables organizations to assess the effectiveness of their marketing initiatives and track campaign performance and measure customer satisfaction with unprecedented accuracy and efficiency.

Financial Analysis

BI and analytics prove invaluable in financial analysis. Organizations can use these tools to consolidate and analyze financial data, identify cost-saving opportunities, detect anomalies or fraud, create sales projections, and optimize budget allocation. In Figure 8.9, a projection is made by analyzing historic sales data and extrapolating potential future sales in units over time. By gaining a comprehensive view of their financial performance, organizations can make data-driven decisions that improve profitability and financial stability.

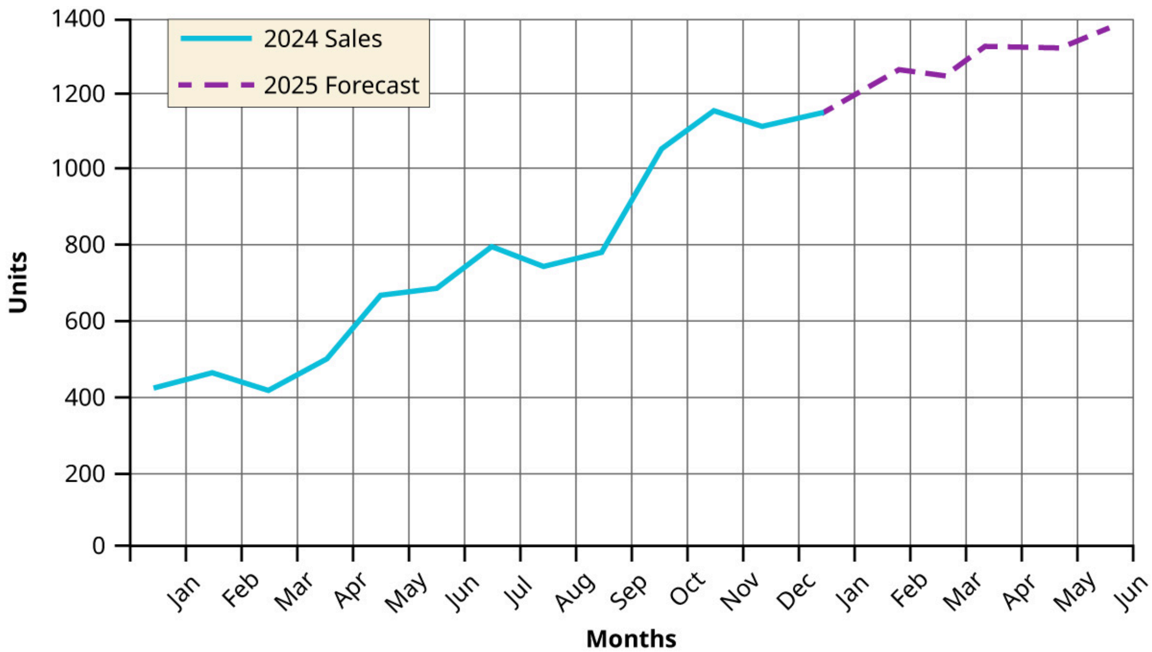


Figure 8.9 A time-series chart can project potential sales based on historical data. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Supply Chain Analysis

The process of supply chain analysis is crucial for optimizing operational efficiency and ensuring timely delivery of goods and services. Business intelligence and analytics enable organizations to track inventory levels, monitor supplier performance, analyze demand patterns, and identify areas for cost reduction and process improvement. Companies can leverage BI to examine the benefits of decisions and identify opportunities to reduce costs using tools such as a **cost-benefit analysis**, which is a systematic approach to assessing the costs and benefits of a proposed project, investment, or decision to determine its feasibility and potential ROI. For example, metrics obtained from the supply chain can help better understand driver behavior and lead to more efficient routes. This data-driven approach enhances supply chain visibility, streamlines logistics, and ultimately improves customer satisfaction. Business intelligence tools enable organizations to transform raw data into actionable insights, empowering them to make informed decisions, adapt to market dynamics, and maximize their potential for success.

Business and Data Analytics Tools

To effectively work with data in the field of BI, you must become familiar with a variety of tools and concepts. There are tools for data storage, data cleaning, data modeling, and data analysis, and techniques for predictive analytics. Two important types of tools are those for visualization and data mining. Visualization tools help with effectively communicating data analysis, and data mining tools help extract meaningful subsets of data for use in data analysis.

Tools for Visualization

Data visualization is a key aspect of data analysis and communication. Effective data visualization not only helps to convey complex information but also aids in decision-making by providing a clear and intuitive understanding of the data.

In terms of modeling and analysis, tools such as Excel, R, and Python can be useful. They provide a wide range of statistical and analytical functionalities that enable users to explore and analyze datasets. Data analytics professionals apply quantitative and qualitative data analysis techniques, understand statistical concepts, and use these tools to build models for predictive analytics and decision support. Today, there are many options for visuals that are typical static charts, but there are also newer interactive charts that allow viewers to explore the data in greater detail or with different parameters. Demonstrations like this can have a strong impact on an audience.

LINK TO LEARNING

To fully understand the capabilities of interactive charts, read this article on some compelling uses of interactivity in data visualization (https://openstax.org/r/109Interactivty) from the Datalabs Agency.

Data Mining

Another important concept, data mining, involves the extraction of valuable information and patterns from large datasets. Data mining can be applied to solve real-world problems and support decision-making processes. One remarkable success story in data mining comes from Netflix's recommendation system. Using a custom algorithm, the streaming company analyzes billions of data points to predict what content a viewer may like.[7]

LINK TO LEARNING

A key component in data analytics involves the mining of data. There are multiple techniques and technical skills commonly needed in this aspect of the industry. Read this article to examine how data science professionals accomplish this (https://openstax.org/r/109DataMining) in more detail.

Professionals who develop proficiency with tools will be able to work with data effectively, conduct quantitative and qualitative analysis, apply data mining techniques, and present findings in a visually compelling manner. This knowledge can further enable you to uncover insights and KPIs, make informed decisions, and contribute to the success of an organization in the field of BI and analytics.

Analytical Models

Several analytical models can enable organizations to gain insights from data and make informed decisions that can lead to overall success. Predictive analytics and BI reporting are two of these powerful tools.

Predictive Analytics

The use of statistical modeling, data mining, machine learning, and other analytical techniques to forecast future outcomes based on historical data patterns is called **predictive analytics**. The key principle is to identify meaningful relationships and patterns within the data that can be used to make predictions. This involves understanding concepts such as training and testing data, feature selection, model evaluation, and accuracy

7 Cyril Shaji, Jayanth MK, Sarah Banadaki, Francisco Quartin de Macedo, and Gladys Choque Ulloa, "What Are Some Real-World Data Mining Success Stories? Netflix and Recommender Systems," LinkedIn accessed January 24, 2025, https://www.linkedin.com/advice/1/what-some-real-world-data-mining-success-stories-gwaqf

assessment.

To learn how predictive analytics works, consider this question: If you study more hours, will your midterm exam score increase? In other words, you want to determine whether there is a positive relationship between the number of hours studied and the score on midterm exams. Although the answer to this question might seem obvious, it is an effective scenario to demonstrate predictive analytics.

To illustrate prediction and regression, suppose the dataset comes from a group of ten people who take a fifty-question exam and provide the number hours they spent preparing for the exam. Each question is worth one point. If you were to chart the results for each participant with the *x*-axis representing the time they spent studying and the *y*-axis representing the resulting grade, it would be possible to generate a visualization like the one in Figure 8.10. This demonstrates regression, which is a statistical analysis method used to quantify the relationship between variables and to make predictions. Note that analysts would typically use regression to form a hypothesis on a dataset that is much larger than our sample population of ten. This smaller example is used for illustrative purposes only.

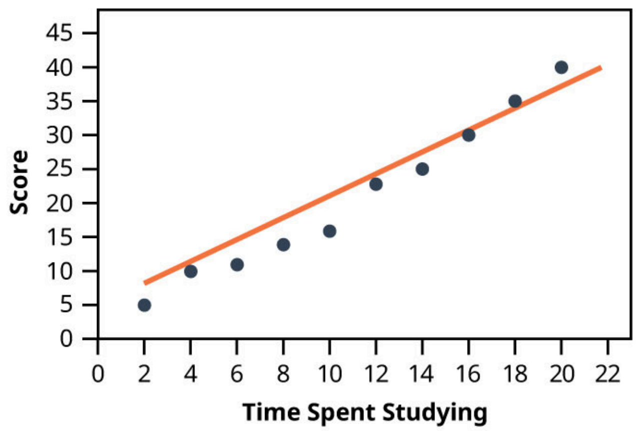


Figure 8.10 This regression analysis shows the results from a hypothetical study exploring the correlation between time spent studying and test scores. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Simple **linear regression** is a method that presents the relationship between variables as a linear equation on a graph, for example, predicting house prices based on features like size, location, and number of bedrooms. It involves plotting *x* and *y* points along a line and determining whether there is a relationship between the variables, and by what margin. If the plotted data follow an upward trend from left to right, there is a positive correlation. Figure 8.10 shows a positive correlation between time spent studying and exam scores.

In a positive correlation, both variables are moving in a positive direction together. There is one dependent variable (the *y*-variable), which is the score on the exam, and one independent variable (the *x*-variable), which is the time spent studying.

There are three important points to remember about linear regression:

- To get an ideal solution, you need data from the whole population. Since that may not be feasible, you could pull a sample to represent the population.
- After acquiring the data, you must choose a relevant model. This can be a daunting task at first but can be done by considering the volume of data, determining whether it is continuous and deciding whether to perform classification or prediction.
- After modeling, you can form predictions.

In linear regression, the term “linear” implies that as the value of one item increases, the other is changing in parallel. Consider the equation for a line: $y = mx + b$, where the following is true:

- y is a dependent variable (outcome). This is the predicted value. In this example, the *y*-variable is the exam score.

- *x* is an independent variable. It is usually time or some other linear value. In this example, the *x*-variable is the time spent studying.
- *m* is the slope of the line.
- *b* is the *y*-intercept value.

In the equation of a line, *y* is a function of *x*. To make a solid prediction, you need to find the values of *m* and *b*. The variable *m* represents the slope of the line, which is the rate of change in the dependent variable (*y*) per unit change in the independent variable (*x*). In simpler terms, it shows how much *y* increases (or decreases) for each additional unit of *x*. So, if *m* is positive, it means that as *x* increases, *y* tends to increase, and if *m* is negative, it means that as *x* increases, *y* tends to decrease.

The variable *b* represents the *y*-intercept of the line, which is the value of *y* when *x* is equal to zero. In other words, it gives the starting point of the line on the *y*-axis.

In the example of time spent studying (*x*) and exam scores (*y*), the slope (*m*) would show how much the grade tends to increase (or decrease) for each additional hour of study time. The intercept (*b*) would represent the grade a student might get if they didn't study at all ($x = 0$).

The variables *m* and *b* are not degrees of correlation but rather parameters that help to define the regression line and understand the relationship between the variables. They provide crucial information about the direction, steepness, and starting point of the line that best fits the data.

In Table 8.1, the values from the study of ten participants with the number of hours studied and the number of correct answers on the fifty-question exam are shown.

x (Hours)	*y* (Score)
2	5
4	10
6	11
8	14
10	16
12	23
14	25
16	30
18	35

Table 8.1 Sample Study Data
In the hypothetical study, the number of hours spent studying correlates positively with the number of correct answers.

x (Hours)	*y* (Score)
20	40
110	**209**

Table 8.1 Sample Study Data In the hypothetical study, the number of hours spent studying correlates positively with the number of correct answers.

After checking some new *x* values (time) to predict the scores, it becomes possible to form a prediction based on new *y* values. Now, you can identify predicted scores and how much they vary from the actual score, expressed in terms of error. Refer to Table 8.2 for the computed values, and view Figure 8.11 for how the predictions would plot on a graph.

x (study time)	*y* (exam score)	$x \times y$	x^2	*y* (predicted score)	Error
2	5	10	4	4.447	0.553
4	10	40	16	8.227	1.773
6	11	66	36	12.007	−1.007
8	14	112	64	15.787	−1.787
10	16	160	100	19.567	−3.567
12	23	276	144	23.347	−0.347
14	25	350	196	27.127	−2.127
16	30	480	256	30.907	−0.907
18	35	630	324	34.687	0.313
20	40	800	400	38.467	1.533
New *x* values					
25				47.917	
30				57.367	

Table 8.2 Predicting Scores and Calculating Error You can determine the error between the actual value and the predicted value, and you can use the existing data to predict scores based on new values.

x (study time)	*y* (exam score)	*x* × *y*	x^2	*y* (predicted score)	Error
35				66.817	
40				76.267	

Table 8.2 Predicting Scores and Calculating Error You can determine the error between the actual value and the predicted value, and you can use the existing data to predict scores based on new values.

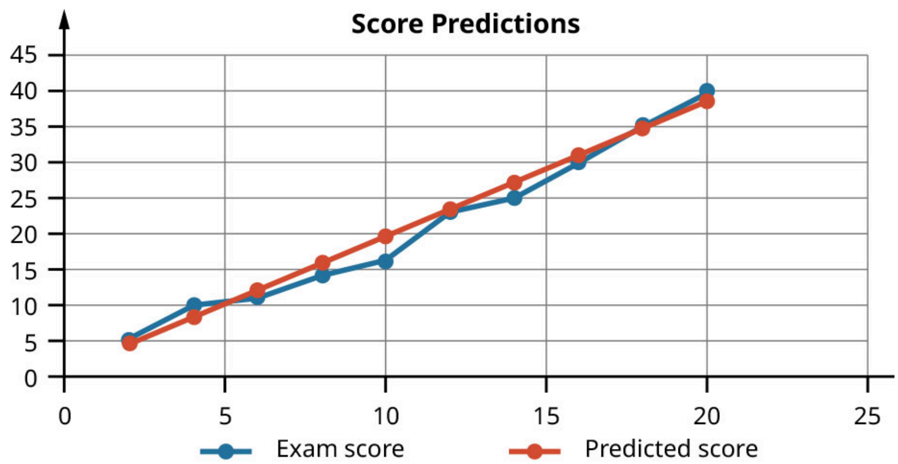


Figure 8.11 Values from the study are plugged in and calculated, forming predicted grades that can be plotted on a graph. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Notice that the values of the predicted score surpassed the maximum score of the fifty-question exam. The implication is that studying thirty hours or more would result in getting a higher than perfect score, which obviously is not possible. This highlights the important fact that no predictive model is perfect. However, the example does demonstrate positive correlation.

Forecasting

To apply predictive analytics techniques, analysts gather relevant information from historical data. Presumably, the more information they gather, the more accurate their model is. The data are gathered and entered in the model in a process called **training**, which uses labeled or historical data to teach machine learning algorithms or models to recognize patterns, relationships, and trends, enabling them to make predictions or classifications on new data. The trained models are then used to make predictions on new, unseen data. Predictive analytics techniques can be applied across multiple disciplines, including sales forecasting, demand prediction, and future stock performance. To perform analysis on historical data, analysts sometimes turn to libraries, or freely available code segments, to augment an algorithm with additional features.

Decision-Making

Predictive analytics tools help stakeholders make decisions. The historical data and associated trends help organizational leaders anticipate future scenarios and make data-driven decisions. For example, predictive analytics can help businesses optimize inventory levels, develop targeted marketing campaigns, optimize pricing strategies, or predict equipment failures to plan maintenance activities proactively. Note that descriptive analytics, diagnostic analytics, and prescriptive analytics are all used as decision-making tools.

Analysis of historical data to gain insights into past events, trends, and patterns within an organization or specific business processes is called **descriptive analytics**. A full descriptive study can also help identify external events that disrupted the data. In the example of a stock price analysis, sudden global events can produce a profound impact, as seen with the COVID-19 pandemic. Descriptive analytics focuses on summarizing and visualizing data to answer questions like the following:

- "What happened?"
- "What are the key trends?"
- "How can we leverage the organization to take advantage of this data?"

The process of examining patterns in data to identify correlations and causes of certain events or outcomes is called **diagnostic analytics**. For instance, in the context of customer attrition, diagnostic analytics might uncover correlations between customer behavior and service quality issues, allowing organizations to address underlying issues more effectively and thereby retain more customers.

The process of using data analysis and modeling techniques to recommend specific actions or strategies to optimize business processes and outcomes is called **prescriptive analytics**. It takes a proactive approach by providing recommendations on the best course of action to optimize future outcomes. It leverages advanced analytics techniques to simulate various scenarios and determine the most optimal decision or action to achieve desired outcomes.

Business Intelligence Reporting

The process of collecting, analyzing, and presenting data in a format that communicates insights derived from BI analysis to support decision-making within an organization is called **business intelligence reporting**. It focuses on transforming raw data into meaningful information and insights through an interactive dashboard, reports, and visualizations. The goal is to provide stakeholders with accurate, relevant, and timely information to support strategic, tactical, and operational decision-making.

CAREERS IN IS

Average Salary for Jobs with Predictive Analytics and Modeling Skills

The field of predictive analytics is experiencing rapid growth, creating exciting career opportunities for individuals with strong analytical and data-related skills. As businesses increasingly recognize the value of leveraging data to make informed decisions and gain a competitive edge, professionals specializing in predictive analytics are in high demand to develop models, forecast trends, and drive actionable insights from vast amounts of data. In 2024, base salaries averaged over $250,000.[8]

Data scientists and analysts play a critical role in designing and developing BI reports. They identify KPIs, define data requirements, select appropriate visualizations, and create reports that cater to the specific needs of stakeholders. This process involves data modeling, report design, and development of data-driven visualizations. Data visualization tools like Tableau, Microsoft Power BI, or custom-built solutions play a vital role in aiding managers in decision-making processes.

Here are several ways in which BI reporting supports managers:

- access to real-time and accurate information
- performance monitoring and KPIs
- data visualization and analysis
- identification of trends and opportunities
- data-driven decision-making

Despite its advantages, BI reporting also has potential disadvantages that organizations may encounter:

8 "Average Salary for Jobs with Predictive Analytics and Modeling Skills," Salary.com, accessed December 11, 2024, https://www.salary.com/research/salary/skill/predictive-analytics-and-modeling-salary

- Implementation can be complex and costly.
- Business intelligence reporting relies heavily on data accuracy, so data quality and successful integration are important.
- Organizations may become overly reliant on technology and infrastructure.
- Business intelligence reporting involves handling sensitive business data, so it is necessary for organizations to maintain privacy and security.

LINK TO LEARNING

Data extraction has been described as the backbone of analytics. The process prepares the data for analysis, transmission, and storage. Read this article from Rivery to examine the process of and types of data extraction (https://openstax.org/r/109DataExtract) in more detail.

Ethical and Legal Aspects of Data Collection

As you learned in 5.2 Security Technologies and Solutions and 6.2 Vulnerabilities and Threats in Web Applications and IoT Technology, ethical and legal considerations surrounding data collection have become increasingly important as organizations gather and analyze vast amounts of data. Further, there have been some ethical concerns with AI in data analytics, such as bias in algorithms and the ethics of data usage without consent. Organizations must prioritize transparency and inform individuals about the purpose of data collection, the types of data being collected, and how it will be used.

This means ensuring the lawful basis for data collection, implementing data retention policies, and providing individuals with the right to access, modify, or delete their data as required by the law. Ultimately, ethical and legal aspects of data collection aim to strike a balance between leveraging data for insights and innovation while safeguarding individual privacy rights and ensuring responsible data handling practices.

ETHICS IN IS

The Rise of Data and AI Ethics[9]

Governmental bodies are showing signs of becoming more socially and ethically responsible regarding ethical data consumption. Leading the way is the EU's GDPR, which enforces tight restrictions. The GDPR was the first organization to give citizens the right to be "forgotten," paving the way for other governments to follow suit. There are obvious advantages of GDPR compliance, but it is critical to be aware of potential drawbacks as well. Challenges include the high cost of compliance, complexity, and the impact on small businesses that may lack resources for full obedience.[10] Other developed countries have created their own oversight groups to enforce data security.

9 Nihar Dalmia and David Schatsky, "The Rise of Data and AI Ethics: Managing the Ethical Complexities of the Age of Big Data," Deloitte Insights, June 24, 2019, https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-data-ai-ethics.html

10 Terence Jackson, "The Pros, Cons and True Impact of GDPR One Year Later," *Cyber Defense Magazine*, July 8, 2019. https://www.cyberdefensemagazine.com/the-pros-cons-and-true-impact-of-gdpr-one-year-later/

8.3 Analytics to Improve Decision-Making

Learning Objectives

By the end of this section, you will be able to:

- Explain the role and importance of analytics in decision-making
- Examine how organizations use business analytics for decision-making
- Apply analytics to the decision-making process

Data analytics is a powerful tool that has revolutionized the way businesses make informed decisions. It involves the systematic collection, interpretation, and analysis of vast amounts of data to uncover valuable insights and patterns. By harnessing the potential of data analytics, organizations can gain a deeper understanding of their operations, customer behavior, and market trends.

Role and Importance of Analytics in Decision-Making

In today's rapidly evolving business landscape, the ability to make informed decisions is paramount to the success of organizations across industries. By leveraging advanced analytical techniques and tools, businesses can transform raw data into actionable intelligence, enabling them to anticipate market trends, optimize operational efficiency, and enhance customer experiences. There are three fundamental analytics methodologies—decision trees, regression analysis, and clustering—that underpin data-driven decision-making processes and offer valuable insights into various aspects of business operations and strategy.

Decision Trees

Decision trees, are commonly used to classify and predict outcomes by splitting the data based on predictor variables if data are discrete. If data are continuous, then the decision may be based on some absolute characteristic, such as whether the value is less than a certain value. For example, a bank can use a decision tree to determine whether to approve or deny a loan application. The tree might split at criteria like credit score, income level, debt-to-income ratio, and employment status. Using a decision tree standardizes the evaluation of an applicant's criteria, automates the process of approval, ensures transparency in the approval process, and allows the bank to make data-driven decisions.

Regression

Another powerful tool in data analytics is **regression**, which is a statistical analysis method used to quantify the relationship between variables and to make predictions. Linear regression is one type of regression. By analyzing historical data and identifying patterns, regression models can forecast future trends and outcomes. This enables businesses to make informed decisions based on quantifiable insights. For example, a retail company can use regression to predict future sales based on several factors, such as the amount spent on advertising, seasonality, and price changes. By using linear regression, the company can model how these independent variables affect sales and make more accurate predictions. The company can also optimize their marketing budget, manage inventory more accurately, determine how price changes can impact sales, and analyze how seasonality affects sales.

Neural Networks

A neural network provides a means of machine learning by establishing a network of thousands or even millions of nodes in a weighted system of forward-moving data. Patterned loosely after biological conceptual models of how humans understand cognition, images are "trained" to provide a basis for pattern recognition. Neural networks are used in customer support chatbots to handle customer inquiries, provide recommendations, and resolve issues. Chatbots that use deep learning can enhance customer experience by understanding natural language and context and by offering personalized responses. They can also improve their accuracy in response generation and ultimately improve efficiency, leading to cost reduction and a faster response time.

Clustering

The unsupervised learning technique used to group similar data points together based on their intrinsic characteristics or attributes is called **clustering**. This approach is valuable for segmentation and customer profiling, allowing organizations to identify distinct groups within their target audience. By understanding these segments, businesses can tailor their marketing strategies, product offerings, and customer experiences to better meet the needs and preferences of each group. Clustering is an effective method to use in health care to improve patient care by segmenting patients based on their medical conditions, lifestyle factors, and response to treatment. The health-care organization would be able to identify groups of patients who share similar characteristics, allowing the provider to tailor treatment plans more effectively and improve outcomes.

Choosing Appropriate Models or Tools

When choosing which models to implement, organizations consider several factors. First, they evaluate the nature of the problem or decision at hand. Decision trees are often used when there are multiple decision paths, while regression analysis is suitable for predictive modeling. Clustering is employed when segmenting data is essential for personalized targeting. Second, organizations assess the availability, quality, and complexity of the data. Some models, like decision trees, provide easily interpretable results, while others, such as neural networks, may offer higher accuracy but are more challenging to interpret. Ultimately, organizations strive to select the most appropriate model that aligns with their goals, data availability, interpretability needs, and computational capabilities.

How Organizations Use Business Analytics for Decision-Making

Organizations use business analytics to make different kinds of decisions, communicate results to stakeholders, and attend to a variety of ethical and social considerations. By leveraging data-driven insights, businesses can improve decision-making across various functions, including marketing, finance, operations, and human relations, ensuring that strategies are informed by the data they collect. Furthermore, business analytics enables organizations to present clear and actionable insights to stakeholders, fostering transparency and trust while supporting informed decision-making at all levels. However, as organizations collect and analyze vast amounts of data, they must also address ethical concerns such as data privacy, bias in algorithms, and the social impact of automation, ensuring that their use of analytics aligns with societal values and regulatory standards.

Operational, Tactical, and Strategic Decision-Making

Analytics play a vital role in helping businesses utilize different decision-making processes, including operational, tactical, and strategic decision-making. An **operational decision** is focused on day-to-day activities and involves optimizing processes, allocating resources, and managing immediate operational challenges. Analysts support operational decision-making by using analytics to monitor KPIs, identifying bottlenecks, and suggesting process improvements. As an example, suppose a retail store manager decides to adjust the store’s inventory levels based on daily sales data and customer demand forecasts. This decision involves managing day-to-day operations such as stocking shelves, replenishing inventory, and scheduling staff to meet immediate customer needs and maintain efficient store operations.

A **tactical decision** is a medium-term decision made by an organization to achieve specific objectives or goals within a defined time frame. These decisions involve resource allocation, budgeting, and setting targets. Analysts assist in tactical decision-making by conducting trend analysis, forecasting, and scenario planning. For example, a marketing manager makes a tactical decision when they launch a targeted advertising campaign for a new product line based on market research, customer segmentation analysis, and competitor benchmarking. This decision would involve developing specific marketing strategies and tactics to achieve short- to medium-term objectives, such as increasing brand awareness, expanding market share, or driving sales growth within a particular market segment.

A **strategic decision** is a long-term decision made by an organization to define its overall direction, goals, and competitive positioning in the market. Strategic decisions involve evaluating market trends, assessing the competitive landscape, and identifying growth opportunities. Analysts support strategic decision-making by conducting market research, competitive analysis, and trend forecasting. For example, consider a CEO of a multinational corporation who decides to enter a new international market by acquiring a competitor or forming a strategic partnership. This decision is based on comprehensive market analysis, macroeconomic trends, geopolitical factors, and long-term business goals. It involves setting overarching objectives, defining corporate strategies, and allocating resources to position the organization for sustained growth and competitive advantage in the global marketplace.

Communicating Results

Analysts use classification and prediction models to communicate results to stakeholders in a clear and understandable manner. Classification models, such as decision trees or logistic regression, are utilized to categorize data into different classes or groups. Logistic regression is a statistical modeling technique used to predict a binary or categorical outcome based on one or more independent variables. Unlike linear regression, it uses the logistic function (sigmoid curve) to model probabilities, ensuring predictions remain between zero and one. For example, logistic regression can be used to predict whether a patient has a disease based on factors like age, blood pressure, and cholesterol levels. It is widely used in classification problems, such as spam detection, customer churn prediction, or medical diagnosis.

These models help analysts communicate findings by presenting the factors or attributes that contribute to a particular classification. For example, in a marketing context, a classification model can be used to identify customer segments based on demographic or behavioral characteristics, enabling analysts to communicate the characteristics that define each segment to stakeholders.

Prediction models, such as linear regression or neural networks, are employed to make forecasts or estimate future outcomes based on historical data patterns. For example, imagine a retail company using a neural network model to predict customer purchasing behavior. By analyzing relevant data, the neural network can learn complex patterns and relationships within the data and then forecast which products customers are likely to buy in the future and anticipate changes in demand. Analysts can present the predicted values or trends to stakeholders so that they can make decisions accordingly.

Ethical and Social Considerations

Ethical concerns relating to handling data for classification and prediction models include using data for legitimate purposes, avoiding biases and discrimination, and ensuring fairness and accountability in the modeling process. Analysts must also remain objectively aware of the potential social implications of their models.

Models can inadvertently perpetuate biases or reinforce existing inequalities if the training data are biased or lack diversity. The human factor is the most important influence over bias and diversity in data. Because humans are responsible for choosing what data are fed into the algorithms and how the results will be applied, unconscious bias may enter the process if the analysts do not pay special attention to the data they use. For example, a NIST study[11] reported that AI facial recognition tools misidentified many people of color.

Analysts should carefully evaluate these biases to avoid negative consequences. Ensuring the ethical and unbiased use of facial recognition technology, especially in areas such as law enforcement, requires a multifaceted approach. Here are some key considerations and strategies analysts can employ:

- Ensure that the datasets used to train facial recognition algorithms are diverse and representative of the population they are meant to serve. This means including a wide range of ethnicities, ages, genders, and other relevant demographic factors in the training data.

11 Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects," NISTIR 8280, National Institute of Standards and Technology, December 2019, https://doi.org/10.6028/NIST.IR.8280

- Implement rigorous testing procedures to detect and mitigate biases in facial recognition algorithms. This can involve analyzing the performance of the algorithm across different demographic groups and identifying any disparities in accuracy rates. Bias mitigation techniques such as algorithmic adjustments, data augmentation, and fairness-aware algorithms can help address these disparities.
- Promote transparency and accountability in the use of facial recognition technology by law enforcement agencies. This includes providing clear documentation on how the technology is used, the potential risks and limitations, and mechanisms for oversight and review by external stakeholders, including civil rights organizations and community members.

Data science professionals play an important role in effectively communicating the results of classification and prediction models to stakeholders, while simultaneously addressing ethical and social considerations to ensure responsible data handling and decision-making.

Case Study: Applying Analytics to the Decision-Making Process

A retail company is considering expanding its product offerings by introducing a new line of clothing targeted at a younger demographic. The decision-makers want to assess the potential success of this new venture and make an informed decision based on data analytics.

1. The first step is problem definition, which involves clearly identifying and defining the problem or decision to be made. In this case, the problem is whether the introduction of a new clothing line for a younger demographic will be a profitable venture for the company.
2. The next step is data collection to support the decision-making process. Data can be obtained from various sources, such as market research and customer surveys. When collecting consumer data for decision-making processes in areas such as market research and customer surveys, it is important to focus on gathering information that directly informs the objectives and goals of the decision-making process. Here is a breakdown of relevant consumer data the company has collected using market research and their own existing customer data:
    - Demographic information: Understanding the demographic characteristics of the target audience, including age, gender, income level, education level, occupation, and geographic location, can help tailor products, services, and marketing strategies to specific consumer segments. The company has determined that in their suburban geographic area there is a large group of potential customers ages sixteen to thirty years who identify among a variety of genders. They are primarily from families at the low to middle income level, and they have some disposable income. The potential customers who are not in high school are in college or are working professionals.
    - Purchase history: Analyzing consumers' past purchase behavior provides insights into their preferences, buying habits, brand loyalty, and spending patterns. This information can help identify trends, predict future purchasing behavior, and personalize marketing messages and product recommendations. The consumers in the company's target audience have some disposable income, so they tend to buy clothing that is on trend and are loyal to popular brands.
    - Psychographic data: Psychographic data delve into consumers' lifestyles, interests, values, attitudes, and personality traits. This information helps marketers understand consumers' motivations, aspirations, and pain points, allowing for more effective targeting and messaging. The company has found that the potential consumers in their region are socially conscious and like to follow trends.
    - Data that might not be as relevant: Collecting demographic data that do not align with the target audience or objectives of the decision-making process may not provide actionable insights and could lead to misinformed decisions. In addition, gathering excessive or irrelevant behavioral data that do not directly correlate with the decision-making goals may result in information overload and detract from actionable insights. Finally, relying solely on anecdotal evidence, unsubstantiated opinions, or speculative assumptions without empirical support may lead to biased or unreliable conclusions and ineffective decision-making.

3. In the final step, the company must perform detailed data analysis to create actionable insights. Analysts can use various techniques such as classification, regression, and clustering (Figure 8.12). For instance, regression analysis can be used to identify the relationship between customer age and purchasing behavior, helping determine the potential demand for the new clothing line. In classification, data points are grouped according to their values, which tend to appear together. In regression, data points are differentiated according to whether they are above or below the line in a regression study. Finally, in clustering, data points are grouped by similarity. For this case study, the clothing retailer used regression and determined that the purchasing behavior of their target audience will likely lead to success in their new clothing line.

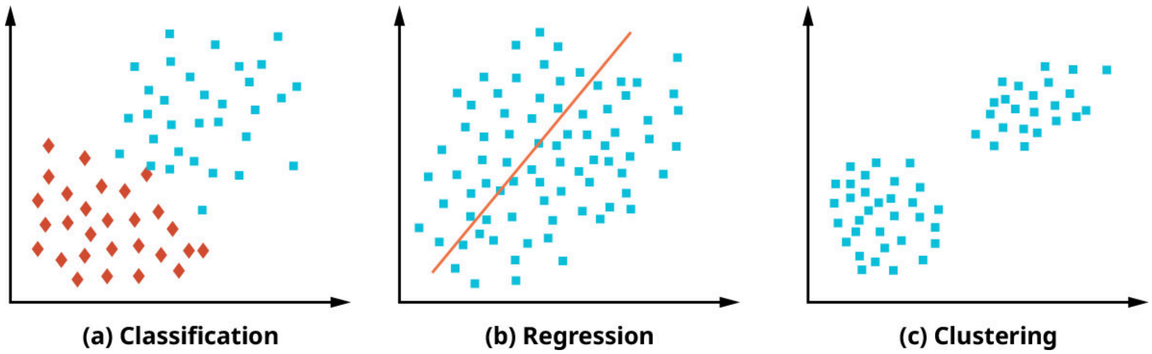


Figure 8.12 Data analysts often use (a) classification, (b) regression, and (c) clustering to help with decision-making. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The company in this case study has done thorough data collection and analysis and determined that there is a market for a gender-neutral clothing line of pants and shirts that is likely to be profitable. The analysts present the data and their conclusions to the stakeholders using some effective visuals, and they agree to move forward with it.

8.4 Web Analytics

Learning Objectives

By the end of this section, you will be able to:

- Explain the role and importance of web analytics
- Examine how web data are collected
- Discuss the web analytics techniques used by businesses to drive site recognition and sales
- Explain search engine optimization

Web analytics is a powerful tool that provides valuable insights into the performance and behavior of websites. The process of **web analytics** involves the collection, measurement, analysis, and reporting of data related to website usage and user interactions to understand and optimize user behavior, engagement, and overall performance. With it, organizations can track various metrics such as website traffic, page views, bounce rates, conversion rates, and user demographics. These metrics enable businesses to gain a deeper understanding of their online presence, user engagement, and marketing effectiveness, such as determining the potential buyer personas and building an understanding of the individuals accessing the website.

The Role and Importance of Web Analytics

With the proliferation of internet usage and the exponential growth of online businesses, the ability to track, analyze, and interpret user behavior on websites has become indispensable. Web analytics provides organizations with invaluable insights into their audience demographics, preferences, and interactions, enabling them to make informed decisions and refine their online strategies. By harnessing the power of data-driven insights, businesses can enhance user experiences, optimize key metrics, and ultimately drive growth and success in the competitive online landscape.

Improving an Organization's Online Presence

Web analytics play an important role in helping organizations optimize their websites and improve their online presence. By analyzing the data obtained, organizations can identify areas for improvement and make data-driven decisions to enhance their websites. For example, through web analytics, organizations can identify pages with high bounce rates and low conversion rates, indicating potential issues in user experience or content. A **bounce rate** in web analytics refers to the percentage of visitors who navigate away from a website after viewing only one page, indicating a lack of engagement or interaction with additional content. A **conversion rate** in web analytics refers to the percentage of website visitors who complete a desired action, such as making a purchase, filling out a form, or signing up for a newsletter.

Based on the data, an organization can make targeted improvements, such as optimizing page load times, enhancing navigation, or refining the messaging on those pages. This knowledge enables organizations to tailor their online strategies, optimize marketing efforts, and create a seamless user experience, ultimately driving higher customer satisfaction and better online performance.

Optimizing Metrics

A **metric** is a quantifiable measure used to track and evaluate the performance, progress, or success of a particular aspect of a business, campaign, or activity. Metrics provide specific data points that can be analyzed to gain insights into how well a website or digital platform is performing. They can include a wide range of measurements, such as website traffic, conversion rates, bounce rates, session duration, and many others. A KPI is one type of metric, for example. These are typically high-level metrics that directly align with the organization's goals and are critical for assessing performance and progress.

The ability to use these metrics to measure website performance and user behavior allows organizations to gauge the effectiveness of their online presence. Web analytics provide insights into KPIs such as the number of unique visitors, page views, average session duration, and conversion rates. These metrics allow organizations to track and measure their website's success over time and compare it against predefined goals and benchmarks. They can also identify opportunities for optimization, refine marketing strategies, and create personalized user experiences based on user preferences and patterns.

Gaining Insights

By using the data from web analytics, decision-makers can gain a comprehensive understanding of their website's performance, identify areas of improvement, and assess the impact of various marketing initiatives or website changes. For example, web analytics can help determine the effectiveness of different advertising campaigns by tracking referral sources, click-through rates, and conversion rates associated with each campaign.

Measured as a percentage, the click-through rate (CTR) tells the viewer how effective an ad is at attracting clicks. The CTR represents the total clicks an ad receives divided by the total impressions, or instances the ad is loaded on a page. A 2 to 5 percent CTR is generally accepted as being successful, but this varies by industry. So if an ad was viewed 10,000 times and was clicked on 500 times, that's a 5 percent CTR. The CTR helps assess the effectiveness of digital marketing efforts. It allows decision-makers to allocate resources effectively and invest in strategies that generate the highest ROI.

GLOBAL CONNECTIONS

Web Analytics Tools Abroad

The methods by which information systems teams analyze web metrics are universal. Techniques include funnel analysis, page view tracking, search engine optimization, bounce rates, and others. However, rules and local practices vary internationally, which begs the question: what tools are used in other developed countries?

In South Korea, a web metric analysis tool that has made waves is Naver Analytics. The project grew out of a search engine tool and now deploys AI-based algorithms to process user behavioral data. In China, a popular tool for web metric analysis is Baidu Tongji (called Baidu Analytics outside of China). Like the popular Google Analytics, the tool requires webmasters to insert some JavaScript code into each page of a website for tracking important KPIs.

Web Data Collection

Different web analytics tools and techniques collect website data using various methods. Here are a few common approaches:

- Page tagging: The method of embedding a snippet of JavaScript code, known as a tracking tag or pixel, on each webpage to track user interactions, behaviors, and events is called **page tagging**. When a user visits the website, the tag sends information to the organization’s analytics tool, which captures data such as page views, clicks, and user interactions. Page tagging is widely used and allows for detailed tracking and customization, as the code can be modified to collect specific data points.
- Log file analysis: Analyzing server log files to gather data on website traffic, user behavior, and server performance, providing insights into website usage patterns and potential issues is called **log file analysis**. Log files record every request made to an organization’s server, including details such as IP addresses, user agents, and accessed URLs. This can provide information about website traffic, user behavior, and errors. However, log file analysis requires expertise in the handling and interpreting of raw log data.
- JavaScript events: Web analytics tools can track specific user interactions through JavaScript events. Any time a user completes an action such as submitting a form or adding an item to a cart, this creates a conversion event. These events are typically tracked using JavaScript code embedded on the website, allowing the organization’s analytics tool to collect data as the events occur.

Web Data Analysis

Data scientists can leverage various web analytics tools and techniques to analyze website data and derive meaningful insights. Some of the common tools include web analytics platforms, data extraction and transformation, statistical analysis and modeling, and custom analysis and visualization tools.

Web Analytics Platforms

Web analytics platforms offer a wide range of features and functionalities to explore and analyze website data. Data scientists can access prebuilt dashboards, reports, and visualizations provided by these tools to gain insight into website performance, user behavior, and conversion metrics. They can segment data based on various dimensions, apply filters, and conduct in-depth analysis using available metrics and dimensions. Additionally, these platforms often offer advanced features like custom event tracking, goal tracking, and e-commerce tracking, enabling data scientists to perform detailed analyses tailored to specific business goals.

Data Extraction and Transformation

Data scientists can extract data from web sources using their APIs or data export tools. Extraction involves removing data, often in multiple forms, from an online source or repository. Frequently, the data file types vary and come in an unstructured form. Extraction makes it possible to filter, organize, and store the data in a common location. Analysts can programmatically retrieve raw data, such as page views, events, and user demographics. To put the data into usable context, it may be helpful to extract data from multiple sources, transform the data into a usable format, and load the data into a data warehouse for data analytics, a process called **extract-transform-load (ETL)** (Figure 8.13). These steps are as follows:

1. Information is extracted from one or more sources and is prepared for transformation.
2. Transformation may involve cleaning up missing or inconsistent data, creating new derived variables, and transforming data into a suitable format for analysis. The data are filtered and organized.
3. The transformed data are loaded into a centralized location.

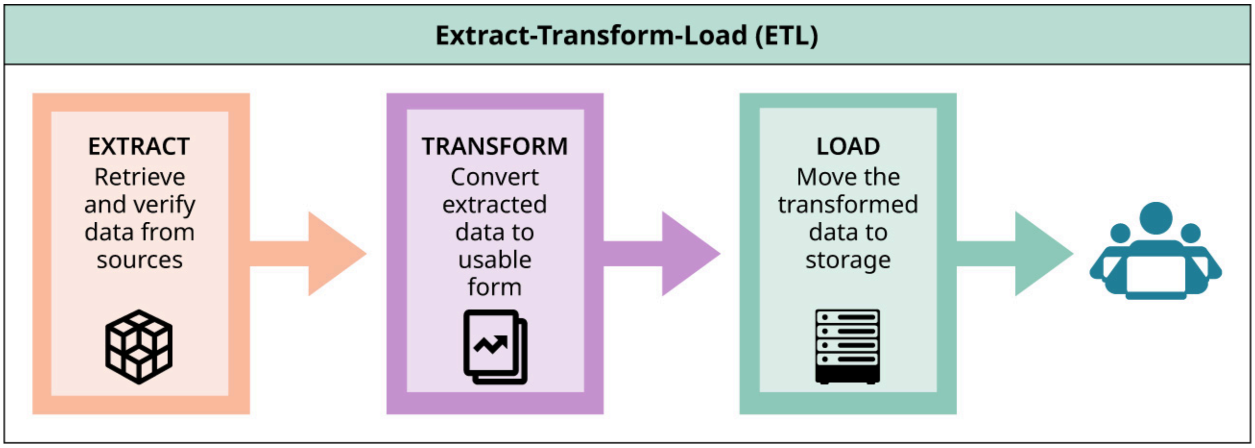


Figure 8.13 ETL is part of the overall workflow for moving data from a database, transforming it, and loading it to a data warehouse for transmission and analysis. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

FUTURE TECHNOLOGY

Self-Service Business Intelligence

Some research suggests that the digital divide appears to be closing. Thanks to self-service ad hoc tools, an increasing number of people can perform tasks previously only possible with the help of professional data analysts and engineers. Historically, data professionals function as “gatekeepers” of the data analysis tools, turning raw data into insightful material. As the name implies, self-service BI provides an opportunity for individuals to proactively derive actionable insights without the need for highly trained professionals to provide oversight.[12] The future of BI may very well eliminate the middleman, allowing executives and other interested parties to run queries, build visualizations, and create dashboards without specialized training.

Statistical Analysis and Modeling

With data that have undergone the ETL process, data scientists can apply various statistical analysis techniques and modeling approaches to gain insights and make predictions. They can use tools like exploratory data analysis classification and customer segmentation.

Exploratory Data Analysis

Exploratory data analysis (EDA) is the process of conducting the initial review of a dataset to spot any patterns or trends early on. Data analysis at this stage looks for relationships between variables. When one feature increases, does another feature do the same? What are the correlations, if any? This initial overview helps data scientists formulate the right questions to ask. Visual outputs can help by providing clues to these relationships. Consider the scatterplot diagram in Figure 8.14. This data from an educational environment recorded student absences and cross-referenced them with the final grade point average (GPA).

12 Michael Segner, “The Future of Business Intelligence,” Monte Carlo, updated January 20, 2024. https://www.montecarlodata.com/blog-the-future-of-business-intelligence/

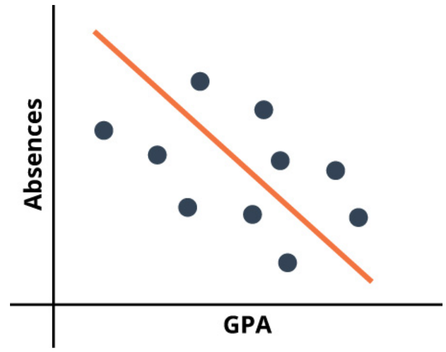


Figure 8.14 Scatterplot diagrams can provide evidence of correlation between features such as absences and GPA. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

You can observe quickly that there is indeed a relationship between the variables of absences and GPA. The lower the absences (the independent variable), the higher the GPA. The trend goes downward and to the right, signifying a negative correlation.

Classification

A scatterplot like the one in the previous example is helpful not only for seeing trends but also for classifying data. One such approach involves clustering, which involves identifying the most relevant characteristics of the data and plotting them out, with the idea being that similar data points will appear to cluster together near the average value, or centroid. Using the iris dataset (refer to 8.1 The Business Analytics Process), you can plot data on petal width (Figure 8.15). For clarity, the apparent clusters are colored differently to communicate the distinctions better visually. For example, the *Iris setosa* data group together in the lower-left portion of the chart and are colored purple.

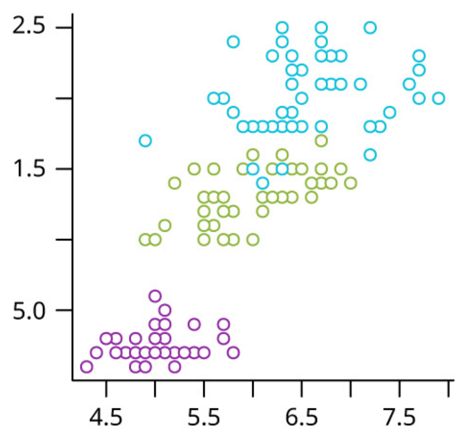


Figure 8.15 In plotting petal width of iris species, the graph reveals three very clear clusters of data. Purple circles = *Iris setosa*; green circles = *Iris versicolor*; blue circles = *Iris virginica*. (source: modification of work "Iris dataset scatterplot" by "Nicoguaro"/Wikimedia Commons, CC BY 4.0)

Customer Segmentation

To better determine how to market goods and services, organizations must understand their audience. By studying customer behavior patterns and other features, organizations can divide customers into groups, which will make the target audience easier to reach. One way is to use *k*-means clustering, which is an unsupervised machine learning algorithm used for clustering data into distinct groups based on similarity. It works by dividing a dataset into *k* clusters, where each data point belongs to the cluster with the nearest mean (centroid). The algorithm iteratively updates the centroids and reassigns data points until the clusters stabilize or reach a convergence criterion. For example, *k*-means can segment customers based on purchasing behavior to identify distinct buyer personas.

Consider an example. Suppose you are tasked with breaking a group of customers down into manageable groups with labels so the marketing team can plan the advertising campaigns more effectively. The first thing you might do is conduct a study that classifies the sample data into age, annual income, and spending score. Spending score is assigned to each member of the study and is based on historic information such as spending habits and other customer behavior (Table 8.3).

CustomerID	Age	Annual Income (in $1,000)	Spending Score (1–100)
1	18	99	58
2	21	43	48
3	19	129	21
4	35	77	29
5	31	86	28
6	24	143	25

Table 8.3 Customer Segment In this example table, customer features are listed in a dataset for analysis. Note that no customer is personally identified. (data source: Zubair Mustafa, "Shopping Mall Customer Segmentation Data," Kaggle, updated April 2024, https://www.kaggle.com/datasets/zubairmustafa/shopping-mall-customer-segmentation-data)

After this, you might perform an EDA to remove outliers. For example, suppose that in the summary statistics, you notice that the average income for consumers aged twenty-five to thirty years is $45,000; however, one data point has a twenty-six-year-old influencer who earns $2.6 million. This will throw off the averages and results dramatically, so that value is excluded. Cleaning the data using the ETL process will make it more accurate and effective for the next stage of the process—analysis and visualization.

Custom Analysis and Visualization

Data scientists can also utilize programming languages such as Python or R to perform custom analysis on the cleaned data. They can leverage libraries and packages specific to web analytics, such as the Google Analytics Reporting API client libraries for Python or R, to access and analyze data programmatically. To gain greater flexibility in conducting advanced analysis, implementing specific algorithms, and creating tailored visualizations to communicate insights effectively, data scientists often write custom code.

Using the data from the customers in your study to help the marketing team, after you clean the data, your next goal might be to identify which characteristics have the most impact on the customer's spending score. You could investigate this by trying to plot age versus spending score (Figure 8.16).

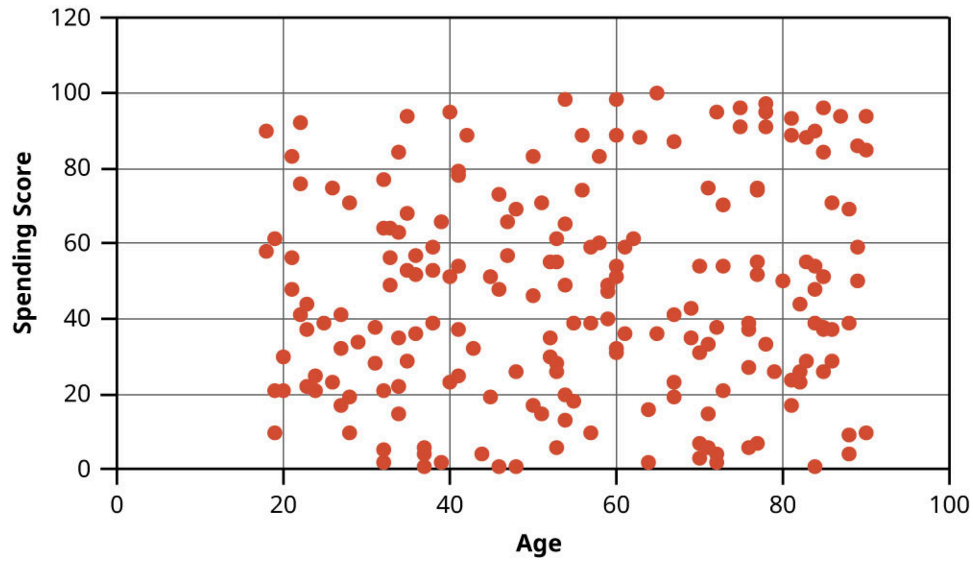


Figure 8.16 Plotting the relationship between spending score and age reveals some groups of customers that may need further analysis. (data source: Zubair Mustafa, "Shopping Mall Customer Segmentation Data," Kaggle, updated April 2024, https://www.kaggle.com/datasets/zubairmustafa/shopping-mallcustomer-segmentation-data; attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Looking at the resulting scatterplot, you can observe that the data seem to be distributed evenly across the whole graph. However, looking more closely, you can see some groups of data, such as a spending score over eighty in people ages seventy to ninety years, a spending score between forty and sixty in people ages forty to sixty years, and a spending score between twenty and forty in people ages twenty to forty years. These distributions likely do not tell the whole story, which can lead you to examine the relationship between age and annual income to determine if that provides any insights (Figure 8.17).

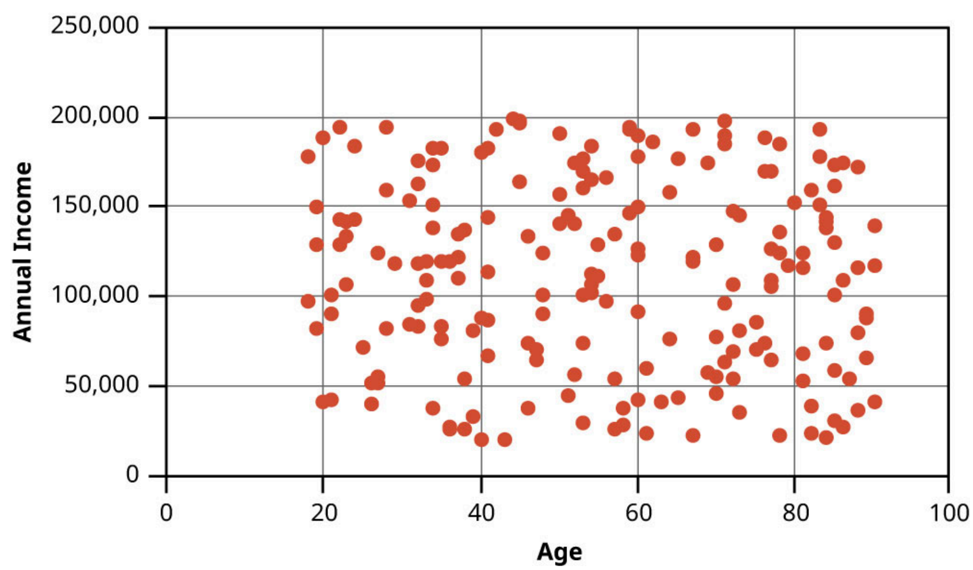


Figure 8.17 Comparing annual income and age in the customer data again reveals several subtle clusters. (data source: Zubair Mustafa, "Shopping Mall Customer Segmentation Data," Kaggle, updated April 2024, https://www.kaggle.com/datasets/zubairmustafa/shopping-mallcustomer- segmentation-data; attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Again, the data here is distributed somewhat evenly across the graph, but there are some clusters of data. The first shows one cluster of people between ages forty and sixty years with the highest annual incomes, between $150,000 and $200,000, and another cluster shows people between the ages of twenty and forty with incomes between $100,000 and $150,000.

With this data in mind, the next step is to examine the correlation between spending score and annual income

(Figure 8.18).

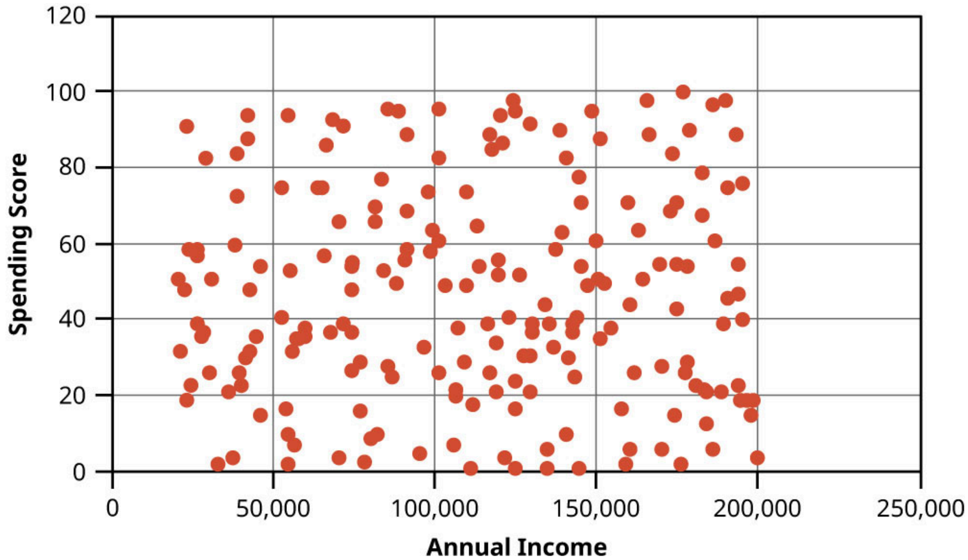


Figure 8.18 Comparing the customers' annual income and spending score reveals additional information that may help to find the best groups to target with a marketing campaign. (data source: Kaggle: Zubair Mustafa; attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Here, there are several clusters of data that give the marketing team a better idea of who their target audience is. Spending score is highest across all income groups but especially for customers who earn $100,000 to $150,000 annually. There is also a cluster of customers ages twenty to forty in that income group, but the customers ages seventy to ninety show a cluster with a higher spending score than those younger customers. These data may be used to show shopping trends, but they do not provide data on what the customers are buying, so the marketing team will need to do some additional analysis on products to further refine their target audience.

This example shows how data scientists can employ web analytics tools and techniques to access, transform, and analyze website data. They can use the tools to uncover meaningful patterns, correlations, and trends, providing valuable insights into website performance, user behavior, and marketing effectiveness. The analysis conducted by data scientists helps organizations optimize their online presence, make informed decisions, and drive business success in the digital landscape.

Search Engine Optimization

Optimizing website content and structure to increase visibility and ranking on search engine results pages is called **search engine optimization (SEO)**. The process involves improving various elements of a website, such as optimizing content with relevant keywords, ensuring proper structure and navigation, acquiring high-quality backlinks, and providing a positive user experience. By following SEO principles, websites can attract more organic traffic and increase their online visibility. In web analytics, “organic” traffic refers to website visitors who arrive at a site through unpaid search engine results, excluding any visits generated from paid advertising or other referral sources.

Identifying Areas for Improvement

Data can be analyzed to uncover insights such as which pages have high bounce rates or low conversion rates or are underperforming. By examining user behavior, traffic sources, and engagement metrics, data scientists can pinpoint specific areas where improvements can be made. These improvements might involve, for example, optimizing landing pages, refining calls to action, or streamlining the checkout process. Web analytics tools provide visualizations, reports, and data segmentation capabilities to support this analysis.

A/B Testing

The method **A/B testing**, also referred to as split testing, is used to compare two versions (A and B) of a webpage, email, or advertisement to determine which one performs better in terms of user engagement or conversion rate. This process randomly splits website visitors into different groups and exposes them to different versions of a page that may have, for example, different headlines, layouts, or calls to action. A **call to action** is a prompt or directive placed within a website, an advertisement, or marketing material that encourages users to take a specific action, such as making a purchase, signing up for a newsletter, or requesting more information.

A/B testing helps identify which elements have a positive impact on user engagement, conversion rates, or other key metrics, and this enables organizations to make data-driven decisions about how to optimize their websites and improve overall performance. This testing can be accomplished by dividing pages into control and variant groups, and the changes can be implemented on either the server side or client side.

On the server side, SEO tests point toward the code itself. The advantage is a smoother and more stable experience for the user. The drawback is its higher complexity, which may require knowledgeable information technology staff to implement and monitor. Client-side testing is deployed with JavaScript coding. There's a slight unsteadiness between the old and new versions of a page. The advantage here is that it is easier to implement. The process does not require hardwiring or specialized training.

LINK TO LEARNING

You can unlock the secrets of effective web design with A/B testing. Discover how to improve approaches to web design, fine-tune layouts, optimize content, and increase conversion rates. Read about how web analytics professionals unlock the potential of a website (https://openstax.org/r/109WebDesign) in this article.

Key Terms

A/B testing (also, split testing) method used to compare two versions (A and B) of a webpage, email, or advertisement to determine which one performs better in terms of user engagement or conversion rate

application programming interface (API) means by which software applications communicate and interact with each other for the purpose of exchanging data and functionality

benchmarking comparison of an organization's performance against industry standards and competing businesses

bounce rate percentage of visitors who navigate away from a website after viewing only one page, indicating a lack of engagement or interaction with additional content

business intelligence (BI) process of collecting, analyzing, and interpreting data to inform business decision-making and improve organizational performance

business intelligence reporting process of creating, designing, and delivering reports and visualizations that communicate insights derived from BI analysis to support decision-making within an organization

call to action prompt or directive placed within a website, advertisement, or marketing material that encourages users to take a specific action, such as making a purchase, signing up for a newsletter, or requesting more information

clustering unsupervised learning technique used to group similar data points together based on their intrinsic characteristics or attributes

conversion rate percentage of website visitors who complete a desired action, such as making a purchase, filling out a form, or signing up for a newsletter, out of the total number of visitors

cost-benefit analysis systematic approach to assessing the costs and benefits of a proposed project, investment, or decision to determine its feasibility and potential return on investment

data analysis systematic process using statistical and logical techniques to review, sort, and condense data for the purpose of gaining insight on areas of interest

data analytics process of examining datasets to draw conclusions and insights, typically using statistical and computational methods to inform decision-making or solve problems

data marketplace online platform or ecosystem where data providers and consumers can buy, sell, or exchange datasets and related services

data mining process of analyzing large datasets to discover patterns, trends, and insights using statistical and computational techniques

decision tree decision-making tool that uses a tree structure diagram in which branches represent choices and their outcomes

descriptive analytics analyzing historical data to understand past performance, trends, and patterns within an organization or specific business processes

diagnostic analytics examining patterns in data to identify correlations and causes of certain events or outcomes

extract-transform-load (ETL) process used to extract data from multiple sources, transform the data into a usable format, and load the data into a data warehouse for data analytics

key performance indicator measurable value that demonstrates how effectively a company is achieving its key business objectives and goals

linear regression method that presents the relationship between variables as a linear equation on a graph

log file analysis analysis examining server log files to gather data on website traffic, user behavior, and server performance, providing insights into website usage patterns and potential issues

metric quantifiable measure used to track and evaluate the performance, progress, or success of a particular aspect of a business, campaign, or activity

operational decision decision focused on day-to-day activities that involves optimizing processes, allocating resources, and managing immediate operational challenges

outlier observation that deviates significantly from the rest of the dataset, potentially indicating anomalies, errors, or unique patterns that require special attention during analysis

page tagging embedding a snippet of JavaScript code, known as a tracking tag or pixel, on each webpage to track user interactions, behaviors, and events

predictive analytics use of statistical algorithms and machine learning techniques to analyze historical data and forecast future outcomes or trends

prescriptive analytics using data analysis and modeling techniques to recommend specific actions or strategies to optimize business processes and outcomes

recency, frequency, and monetary (RFM) task of customer segmentation or grouping based on their purchasing habits

regression statistical analysis method used to quantify the relationship between variables and to make predictions

search engine optimization (SEO) process of optimizing website content and structure to increase visibility and ranking on search engine results pages

sensor data collection gathering data from sensors designed to detect and respond to physical or environmental conditions, such as temperature, pressure, or motion

strategic decision long-term decision made by an organization to define their overall direction, goals, and competitive positioning in the market

tactical decision medium-term decision made by an organization to achieve specific objectives or goals within a defined time frame

training process that uses labeled or historical data to teach machine learning algorithms or models to recognize patterns, relationships, and trends, enabling them to make predictions or classifications on new data

visualization graphical representation of data and information to facilitate understanding, analysis, and communication of insights and trends

web analytics collection, measurement, analysis, and reporting of website data to understand and optimize user behavior, engagement, and overall performance

web scraping automated extraction of data from websites, typically using software to simulate human browsing behavior and retrieve information from web pages

Summary

8.1 The Business Analytics Process

- Analytics 1.0, 2.0, and 3.0 are three distinct eras in the evolution of big data. The current era is Analytics 3.0, which uses traditional analytics to analyze big data. Big data allows organizations to gain a comprehensive understanding of their target market and customer base.
- Challenges of working with big data include its volume, its quality, governance of the data, and the extraction of actionable insights.
- The collection of big data occurs through web scraping, sensor data collection, social media, data marketplaces and APIs, and internal data sources.
- The business analytics process involves defining the problem, preparing the data, running statistical analysis, interpreting the results, and implementing changes.

8.2 Foundations of Business Intelligence and Analytics

- With BI, organizations can identify trends, patterns, and correlations to understand customer behavior, market dynamics, and operational performance.
- Organizations harness BI to gain an edge with tools to aid in marketing, predictive analytics, and financial analysis.
- Business and data analysis tools include tools for visualization, data mining, and predictive analytics.
- Business intelligence reporting focuses on transforming raw data into meaningful information and insights through interactive dashboards, reports, and visualizations.

- Organizations that collect and store data must adhere to legal and ethical guidelines to balance the protection of individuals' privacy with the usefulness of the data.

8.3 Analytics to Improve Decision-Making

- Data analytics involves the systematic collection, interpretation, and analysis of vast amounts of data to uncover valuable insights and patterns.
- Analytics tools such as regression, decision trees, and clustering models aid in deriving actionable data.
- Regression is a statistical method used to analyze the relationship between one dependent variable and one or more independent variables.
- Decision trees split the dataset into subsets based on the most significant attribute at each step.
- Clustering models group similar data points into clusters based on certain features or characteristics.
- Analysts need to consider ethical and social considerations and ensure compliance with privacy regulations and protect sensitive information.
- Using these techniques in the decision-making process can lead to greater chances of success in business.

8.4 Web Analytics

- Web analytics is a powerful tool that provides valuable insights through the collection, measurement, analysis, and reporting of data related to website usage and user interactions.
- Web analytics tools collect data through page tagging, log file analysis, JavaScript events, and cookies.
- Businesses leverage various web analytics techniques to enhance site visibility and drive sales, highlighting the pivotal role of data-driven insights in optimizing online strategies and fostering customer engagement for improved performance.
- Web analytics tools provide insight into customer behavior, opportunities for improvement, and bounce rates.
- Incorporating SEO into an organization's web analytics strategy enhances visibility and drives organic traffic by optimizing keywords, improving site rankings, and analyzing user engagement metrics for targeted content refinement.

Review Questions

1. What is an accurate definition of data analytics?
   a. the process of collecting and storing large volumes of data
   b. the practice of examining, cleaning, and transforming data to uncover insights
   c. the use of statistical methods to forecast future market trends
   d. the integration of structured and unstructured data into a centralized database

2. What does the term "big data" refer to?
   a. a collection of data that is too large to be processed by traditional methods
   b. a dataset with high accuracy and reliability
   c. a dataset that contains only structured data
   d. the process of analyzing data to uncover hidden patterns and trends

3. What is one of the significant challenges associated with big data collection and use?
   a. lack of available data sources
   b. slow processing speed
   c. insufficient storage capacity
   d. data volume, velocity, and variety

4. What is the final stage of the business analytics process before the cycle begins again?
   a. results interpretation
   b. statistical analysis
   c. implementation

d. data preparation

5. What are some benefits of implementing business intelligence in an organization?
   a. streamlined decision-making, improved efficiency, and enhanced data security
   b. increased satisfaction, reduced employee turnover, and improved supply chain management
   c. enhanced data visualization, improved data governance, and increased data storage capacity
   d. higher market share, improved brand awareness, and increased sales revenue

6. How do organizations typically use business intelligence in marketing and decision-making?
   a. to remove outliers in customer data
   b. to automate sales processes and improve customer relationship management
   c. to monitor and analyze competitors' pricing strategies and adjust pricing accordingly
   d. to forecast future market trends and make data-driven strategic decisions

7. What is the primary purpose of data visualization in the context of business intelligence?
   a. to present data in an aesthetically pleasing manner
   b. to summarize complex data and highlight patterns or trends
   c. to ensure data security and protect sensitive information
   d. to store and organize large volumes of data for future analysis

8. What is the primary goal of business intelligence?
   a. to gather and store large amounts of data offline
   b. to analyze data and generate insights for decision-making
   c. to identify and address data quality issues
   d. to classify data

9. What key principle underlies predictive analytics?
   a. visualizing historical data patterns
   b. summarizing and visualizing data for decision-making
   c. identifying meaningful relationships and patterns within data
   d. simulating various scenarios to optimize future outcomes

10. In decision tree analysis, what is the purpose of the nodes in the tree structure?
    a. to represent the outcome or target variable
    b. to split the data based on the predictor variables
    c. to display the probability of each outcome
    d. to calculate the information gain

11. What is clustering in data analytics?
    a. a technique for predicting future outcomes based on historical data
    b. the process of identifying relationships between variables to determine cause and effect
    c. a method for categorizing data into groups based on similarities
    d. an approach for analyzing data to uncover patterns and trends

12. What type of decision-making process focuses on long-term decisions that shape the overall direction and future of the organization and includes evaluating market trends and identifying growth opportunities?
    a. operational decision-making
    b. tactical decision-making
    c. strategic decision-making
    d. classification decision-making

13. What step in the data-driven decision-making process involves using techniques such as classification, regression, clustering, and association analysis to uncover patterns and trends within the collected data?
    a. problem identification

b. data collection
c. interpretation of analytics
d. data analysis

14. What description best describes the role of web analytics in organizations?
a. identifying opportunities for improvement
b. enhancing offline performance
c. decreasing user experiences
d. making subjective decisions

15. What can organizations measure using web analytics?
a. emotional responses of users
b. physical sales in brick-and-mortar stores
c. the impact of marketing campaigns
d. the color scheme of their website

16. What web analytics method involves placing a small piece of JavaScript code on each webpage to capture data such as page views, clicks, and user interactions?
a. log file analysis
b. cookies and user identification
c. JavaScript events
d. page tagging

17. What is the primary purpose of A/B testing in website optimization?
a. to optimize website content with relevant keywords
b. to analyze user behavior and traffic sources
c. to compare and determine which web page variation performs better
d. to acquire high-quality backlinks for the website

Check Your Understanding Questions

1. What are some of the challenges associated with collecting and using big data, and how can organizations address these challenges to unlock the full potential of big data for strategic decision-making?
2. In what ways can businesses use big data to gain a competitive advantage and improve their operations? Provide specific examples from the text to support your answer.
3. Describe the key steps involved in the process of predictive analytics and forecasting, highlighting the main considerations and challenges that organizations face when implementing these techniques.
4. How do organizations choose which analytics model to implement?
5. Describe tools used in web analytics to collect data.
6. How can search engine optimization help an organization differentiate itself from others?

Application Questions

1. Reflect on the role of big data. How has the use of data analysis tools and techniques improved market analysis dynamics? Discuss specific examples where interactions online produce data points of interest to marketing teams.
2. Provide an example from your own experience or knowledge of how predictive analytics and simple linear regression could be applied in a real-world scenario to make informed decisions or predictions.
3. Develop a presentation (three to five slides) describing ways in which organizations utilize forecasting to pursue their company’s goals. Describe the tools they would use and how to explain the results best

visually.

4. Reflecting on your personal data and online interactions, what types of information about yourself would you feel comfortable sharing with organizations, and what boundaries or concerns do you have regarding the data you provide? Consider how your comfort levels may vary across different contexts, platforms, and purposes of data collection.

5. Develop a short (around three minutes) YouTube-like video explaining the best practices for search engine optimization.

9

Information Systems Project Management

Figure 9.1 Project management is a fundamental component of information systems. (modification of work “wocintech stock - 170” by WOCinTech Chat/Flickr, CC BY 2.0)

Chapter Outline

Introduction

Project management is a fundamental component of IS and nontechnical projects. The history of information technology (IT) project management can be traced back to the 1950s, when huge computer systems were designed to be used by the government. As computer systems became more complex, formal project management practices emerged, such as a technique called the critical path method and the Program Evaluation and Review Technique.

In the 1970s, project management became more structured with the development of standards such as the Project Management Body of Knowledge (PMBOK) created by the Project Management Institute (PMI). These standards enabled the profession to explode in the 1980s, and the establishment of the Project Management Professional certification further fueled this expansion. Since then, IT and IS project management has become a career many professionals with IS expertise choose—and businesses are eager to employ them.

Today, IT and IS project management is one of the fastest growing professions in the world. It brings together the elements of IS—such as hardware and software, data management, information security and risks—with steps to keep the team and product in scope, on budget, and within schedule. With the emergence of new software, technologies, and methodologies, businesses need effective project management to optimize complex capital projects, strategic operational initiatives, and day-to-day operations.

9.1 Foundations of Information Systems Project Management

Learning Objectives

By the end of this section, you will be able to:

- Identify concepts, skills, and techniques associated with project management
- Distinguish between project management, program management, and portfolio management
- Apply project management, program management, and portfolio management skills

Project management is a fast-growing field. Businesses are complex and intricate systems that aim to provide products and services to their clients or customers. Project management is an aspect of business systems that provides specific tools and best practices to manage and lead the business. Project management focuses on people, assets, money, and time, and project managers use people, assets, money, and time to lead and manage initiatives that provide the products and services a business sells to its customers. In project management, an initiative, task, or activity is categorized as a project regardless of its complexity and who might oversee its implementation. For example, a task as simple as purchasing new phones or computers for employees can be categorized as a project because phones and computers are critical components of modern-day business and the process of purchasing has a time limit. Without these items, the business would probably not operate.

Concepts and Methodologies of Project Management

The **Project Management Institute (PMI)** is the main accrediting body for the project management process and certifies project managers, program managers, and portfolio managers. The PMI promotes the use of a structured, process-based approach to managing projects. The **Project Management Body of Knowledge (PMBOK)**, developed by PMI, is a guide for handling projects using a systematic methodology and proven processes for initiating, planning, executing, managing, monitoring, and closing a project. PMBOK will be the basis for much of the project management foundations covered here.

Overall **project management** describes the use of specific knowledge, skills, tools, and techniques to provide guidance through each stage of a project. Project management involves planning, organizing, and controlling resources—such as people and materials—to achieve specific goals or objectives within a defined timeline. The person responsible for leading the efforts to plan, organize, and control the resources using various tools and techniques to initiate, plan, execute, monitor, control, and close projects is called a **project manager (PM)**. A **project** is a temporary initiative or endeavor to create a product, service, or result that has beginning and end dates. “Temporary” in this sense only means that a project must have a beginning and an end; it does not refer to the length of the project Figure 9.2. Expanding sales into a new market segment, developing an information system to manage an internal process, opening a new branch of the enterprise, and implementing disaster recovery after a system or security failure—these are all examples of projects.

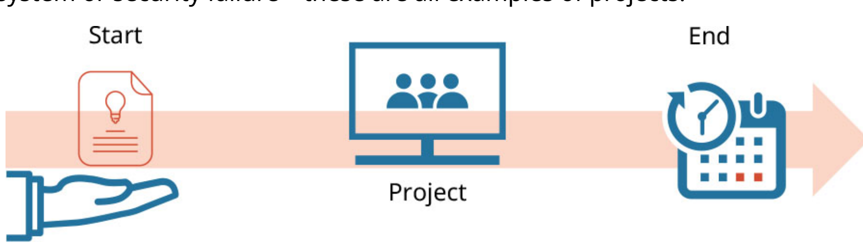


Figure 9.2 A project must have a start date and an end date. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license; credit left: modification of work “Hands collection - star on hand - The Noun Project” by “icon4yu”/Wikimedia Commons, CC BY 3.0; credit left: modification of work “Idea/report icon” by “hidayat, ID, from The Noun Project”/Wikimedia Commons, CC BY 3.0; credit middle: modification of work “Online meeting (the Noun Project 1029565)” by Ismael Ruiz, from The Noun Project/Wikimedia Commons, CC BY 3.0; credit right: modification of work “Countdown (50361) - The Noun Project” by “Icons8”/Wikimedia Commons, CC0 1.0)

A project can follow any timeline, lasting a week, a month, or many years, for example, as long as it meets the definition of a project. A project is considered completed once the scope or requirements have been met or once the objectives of the project have been achieved in accordance with the customer, sponsor of the project, or internal champion of the project. Projects can vary depending on the industry or the environment in which the projects are conducted. For example, a research institution might conduct research projects on new ways to upskill its workforce, while a pharmaceutical company might conduct a project on a new drug to cure Alzheimer's. In the IS field, most projects involve technology and thus are considered technical in nature. An IS project manager might be involved in integrating a new technology into a university's student information system or producing a new process to build electronic vehicles for a car manufacturer.

Project management is used in some form in many organizations. It crosses over many disciplines like construction, business, health care, manufacturing, and other industries where businesses initiate projects that need to be managed by an expert (project manager) who can ensure the project stays within budget, scope, and schedule. A project manager is a key employee with skills in leadership, management, project management, human resources, finance, procurement, contracts, and operations.

Differences Between Project Management, Program Management, and Portfolio Management

Program management and portfolio management can be thought of as managing groups of projects. The coordinated organization, direction, and implementation of a group of related projects is called **program management**. This related group of projects seeks to achieve outcomes and realize benefits that are strategically important to the business. Being coordinated means there are common rules to manage each project, such as when to escalate an issue or that all documentation for each project is similarly organized to group the projects together within the business. A portfolio is simply a collection of projects or programs that are grouped together but may not be interdependent of each other. Usually, these projects are grouped together to more effectively manage the projects based on the business objectives. Therefore, **portfolio management** is the centralized management of a set of projects grouped together to identify, prioritize, authorize, and control the related work Figure 9.3.

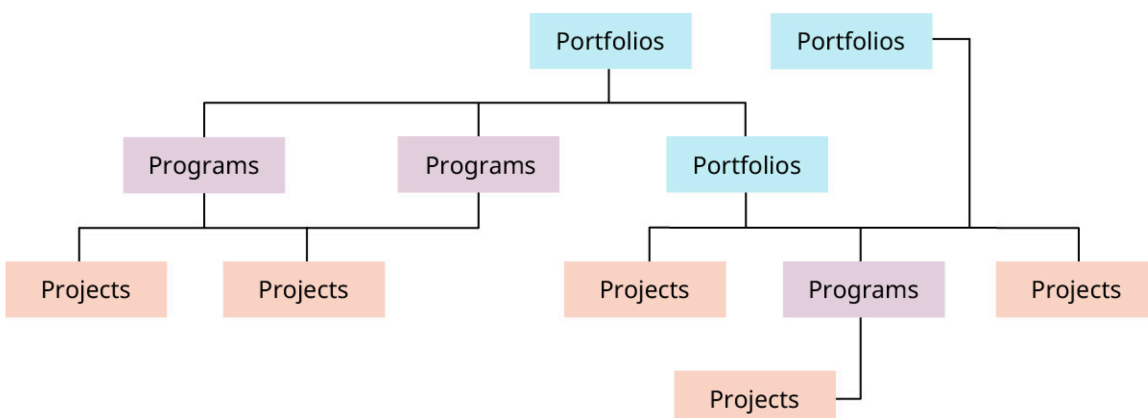


Figure 9.3 In portfolio management, programs or projects are grouped together to realize more efficiency between those programs or projects. Program management groups related projects together to realize a similar outcome for the business. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Understanding project management begins with understanding the underlying principles of the various methodologies used to manage projects. The PMI developed the PMBOK framework and certifies Agile and PRINCE2 frameworks. Each of these frameworks and their supporting methodologies have certain principles that impact how projects are managed. The one thing they have in common is that they all come with documentation, best practices, and processes for managing teams, assets, and deliverables, and they have a very prescribed way to measure the success of each component.

Project management has many different components, complexities, and concepts to support the organization and success of projects. In most IS project management organizations, there is a hierarchical organization of the project management profession, similar to the various management and leadership levels found in health care, marketing, technology, finance, and higher education. Even though the structure is hierarchical, the team supporting the managers and leaders does not always report to the manager or leader of that department.

Project Management Using Project Management Body of Knowledge

The PMBOK is a waterfall approach, which means that each step is followed by the next step, which is followed by the next, and so on. While the sequential design of project steps is central to PMBOK, newer versions of the methodology emphasize that some concepts, such as risk, are more iterative (or repeated), and they must be revisited or monitored frequently.

In PMBOK, the development, monitoring, and control of a project is called the **project life cycle (PLC)** (Figure 9.4). The PLC is a sequence of phases that a project encounters as it progresses from start to finish. The phases include the following:

- Feasibility: In this phase, it is determined whether the organization has the capability to deliver the product.
- Design: This is the planning and analysis phase.
- Building: This phase covers the actual implementation of the project and its project plan.
- Testing: After building the project, the processes must be tested. In this phase, a quality review and inspection of the deliverables are conducted.
- Deployment: With the other phases in the process complete, the project can be deployed. This is when all deliverables are finalized and transitioned to sustainability.
- Closing: In this phase, all the knowledge and artifacts related to the project are archived, and the team members are released.

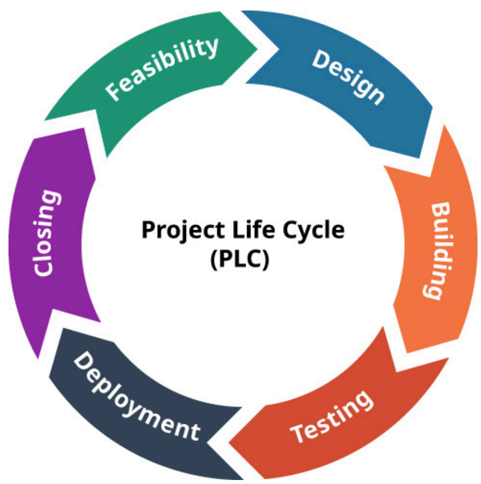


Figure 9.4 The project life cycle is a series of phases that a project goes through from start to finish. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The PMBOK also defines eight domains that guide project managers through the PLC (Figure 9.5). The domains are defined as what the project manager must focus on in each stage to complete that stage. These eight domains ensure successful delivery of the project:

- Stakeholders: Anyone involved or impacted by the delivery of the projects is a stakeholder.
- Team: People who are stakeholders but also invested in the project deliverables are part of the team.
- Development approach: This is the manner in which the phases of the project are planned.
- Planning: The focus of planning is the organization of the project and how it is going to be implemented.
- Project work: The project work includes the necessary items and processes of each deliverable in the project.
- Delivery: This is the actual transition of the project deliverables to the stakeholders.
- Measurement: Measurement includes determining whether the performance of the project and the people are delivering within an expected quality level.

- Uncertainty: The focus of this domain is management of the risks associated with the project.

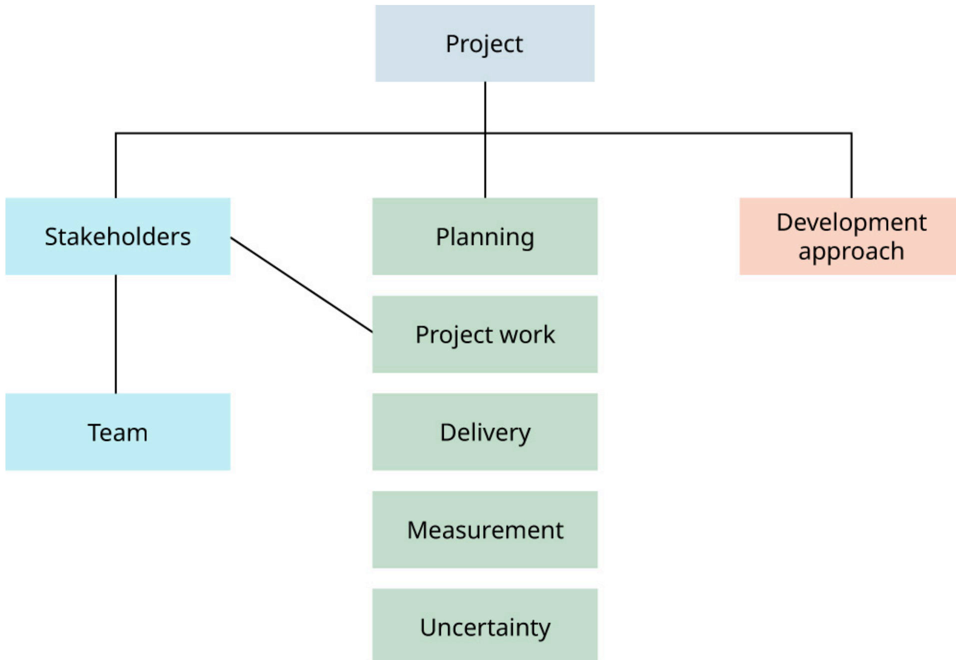


Figure 9.5 The eight domains of performance are what the project manager must focus on in each stage to complete that stage. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Let's look briefly at some domains—stakeholders, team, development approach, and planning—to understand what it means to deliver a project on time within scope, on budget, within acceptable quality levels, and with minimal risk.

Stakeholders' Domain

The stakeholders' domain is a lot about communication and ensuring a good relationship is established with all the individuals associated with a project. Stakeholders include individuals, groups, or organizations that may affect, be affected by, or perceive themselves to be affected by a decision, activity, or outcome related to a project, program, or portfolio. A project's stakeholders could include members of the organization's leadership team, customers, clients, coworkers on the project team, middle management, vendors, regulatory bodies, steering committees—the list goes on and on. Communication and relationships with all stakeholders throughout the project are important to the success of the project. The stakeholders on a given project may shift over time, so keeping up with the list of individuals and groups can be challenging.

In the stakeholders' domain, three desired outcomes should be pursued:

- maintaining a productive relationship throughout the project
- making sure stakeholders are in agreement with the project objectives
- ensuring that stakeholders, who are beneficiaries, are supportive of the project and do not negatively impact project outcomes, such as trying to change the scope of the project or vetoing budget items important to the project

It is important to manage the stakeholders and their expectations both positively and negatively. For example, you could have a stakeholder who has not clearly understood the scope of the project and has additional requirements that are not included in the scope. As the project is developed and the project does not include these items, the stakeholder then believes the requirements have not been met. These expectations and beliefs must be identified as soon as possible.

One way to manage stakeholders is to perform a stakeholder analysis. A **stakeholder analysis** is a review and evaluation of each stakeholder, their background, expertise, and impact on the project. It involves a systematic gathering of quantitative and qualitative data to determine whose interests in the project should be a priority. The stakeholder or group of stakeholders whose interests are a priority are likely to have more power and authority over the project than other stakeholders. These stakeholders are the ones to assure, so it's also important to make sure they are informed and satisfied throughout the project.

Team Domain

The team consists of the individuals who are responsible for building or producing project deliverables. If team members don't work well together, it reflects poorly on the project manager. In fact, it is the project manager's job to create a work environment in which team members work to ensure that deliverables are of high quality and are delivered on time and within budget, with minimal risk. The successful outcome of the project is dependent on the project team and its performance. The need for communication and relationship building among diverse team members is one of the reasons a project manager must be a good leader and communicator in addition to knowing when to push and when to let the team manage its own accomplishments. Establishing a shared-team mindset when it comes to deliverables, quality, and timelines is the goal of the project manager.

Development Approach and Life Cycle Domain

There are many different approaches to **project development**, which is the process of planning a project and ensuring it has the resources necessary to successfully achieve its goals and objectives. The approaches to the PLC highlighted by PMBOK are predictive, adaptive, and incremental development (Figure 9.6).

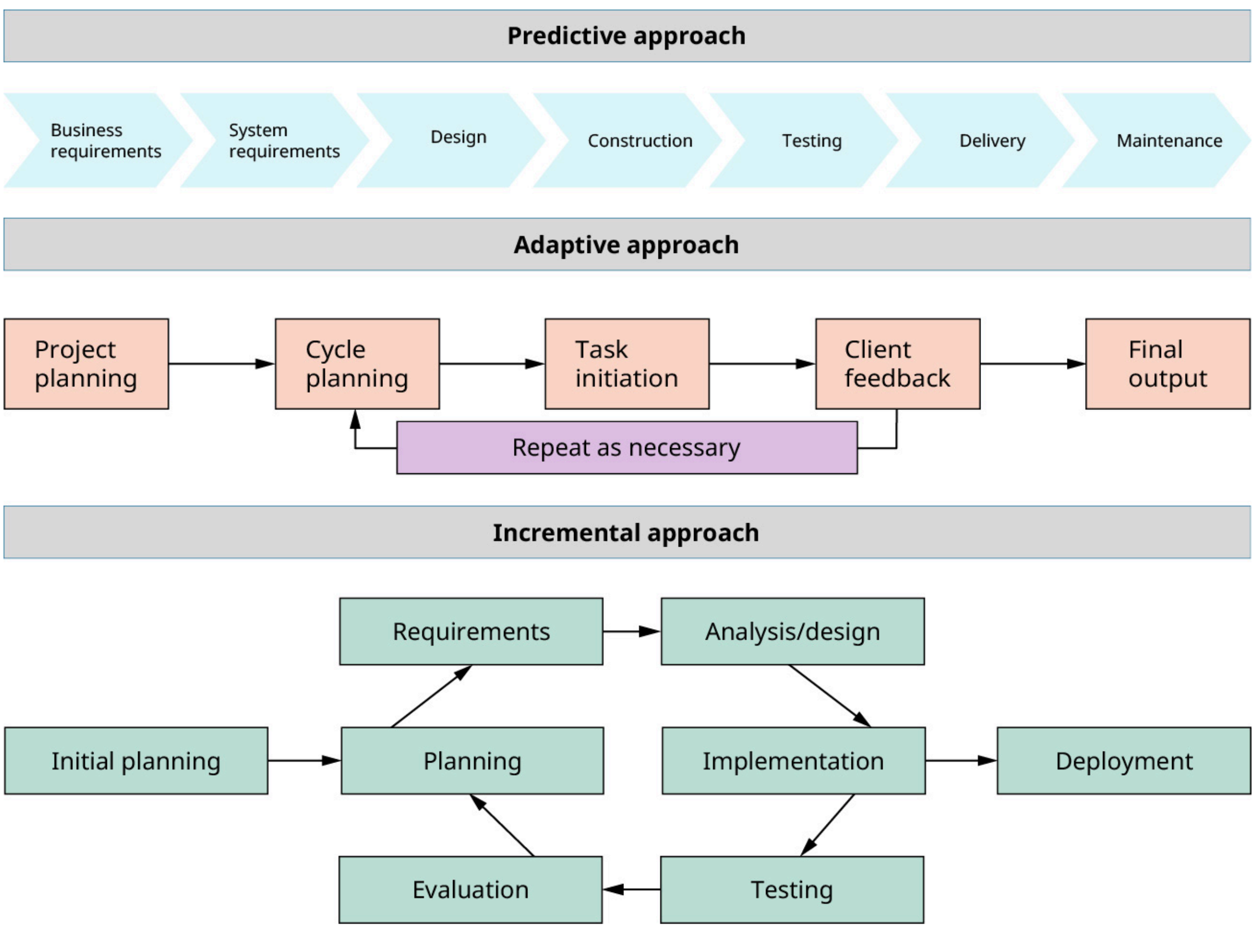


Figure 9.6 The predictive, adaptive, and incremental approaches to project development provide frameworks to develop different types of projects depending on an organization's culture and specific project needs. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The **predictive development approach** is generally used for projects that have specific requirements with well-defined goals and objectives. The entire project is planned from start to finish before the project begins, and once the project is implemented, the plan is followed carefully. This includes adhering to the scope of work and project deadlines to meet requirements, design, construct, test, and deliver outputs according to plan.

When a project needs more flexibility, the **adaptive development approach** provides a framework that enables project team members to repeat the processes of cycle planning and task initiation as needed. This provides an opportunity to respond to client feedback and make changes in the project requirements as part of the ongoing processes. As they repeat the processes, team members are expected to learn by doing and then apply their new knowledge to improve the final project outputs.

The **incremental development approach** enables a project to be divided into parts, or increments, that work together and build on each other to accomplish the overall project. Dividing a project into smaller parts makes each part more manageable. Typically, as each part of the project is done, the project team delivers the outputs for that part, providing an opportunity for feedback on the project's progress. This allows for changes to be made as each part of the project is completed, ensuring that the final product meets the overall project goals and objectives.

Each approach selected depends on the type of project, company culture, organizational structure, organizational capabilities, size of the team, and the location of the team. The workplace culture of the company or your stakeholders' characteristics may dictate the development approach. When it comes to project management, there is never a one-size-fits-all approach. There are many factors to consider, and the approach and PLC can vary from project to project.

Depending on the needs of the project and the culture of the organization, an iterative approach could involve a hybrid method with modifications as needed to fit the project. Another consideration when deciding which approach to use is the degree of innovation involved in a project. This refers to how much change a project introduces. Some projects are minimally innovative, offering incremental changes, while others are more radical, offering changes that are disruptive and even transformative to operations or products.

For example, you may have a project that is very lengthy in duration with lots of interdependencies where the product must be delivered before the next process or components can be built. Say you are leading a project to build a space shuttle. There would be several components that would need to be developed prior to others, but there are some parts that can be delivered in conjunction with each other, like the engines and the capsule for the payload. You can develop the engines while you are developing the capsule because they are not necessarily dependent on each other. The engines are dependent on the weight of the payload, and the capsules can be developed to deliver up to the maximum payload. You could use a predictive approach or even an incremental approach for delivery.

Planning Domain and Project Work

The planning domain lasts throughout the length of the project and is associated with organizing, collaborating, and elaborating on the project and the project deliverables. The project work domain is about the execution of the project. It involves ensuring that the performance of the team and the product or service and the outcomes maintain the appropriate quality and map to the desired outcomes of the project. Each project requires the project manager to plan, coordinate, and manage the project in a holistic approach. No two projects are ever alike.

As a project progresses, there is always a certain amount of feedback and information that needs to be assessed for its impact on the project and its outcomes. Each project will evolve over time. The process of determining the appropriate information to provide to the team needs to be handled and managed to achieve the desired outcomes. The time spent planning for a project and the desired outcomes should be appropriate to the project. Project planning and the project management documentation should always be sufficient to manage stakeholder expectations. There are several project management tools and documents that project managers use in the planning process, such as a vision statement, project charter, business case, initial project plan, or RACI (responsible, accountable, consulted, and informed) charts.

LINK TO LEARNING

Consider this case study (https://openstax.org/r/109CaseStudy) that discusses how extensive planning was used to address the disaster of roads being destroyed after a catastrophic weather event in British Columbia. This example illustrates how the tools and techniques of project management can be used in the professional and personal domains.

Agile Project Management

The **Agile project management** methodology involves taking an iterative and incremental approach to delivering projects (refer to 4.1 Systems Analysis and Design for Application Development for more about Agile methodologies). This means that instead of trying to plan and execute an entire project up front, the project manager breaks the project down into smaller, manageable tasks. Project management teams using the Agile method seek to deliver value incrementally and iteratively by delivering products frequently and engaging with customers to gather feedback. This feedback is then incorporated into the project's direction and objectives immediately. The Agile approach ensures that the final product aligns closely with customer needs and provides maximum value, meaning that the product delivers on the customer's requirements and vision. This approach is particularly good for projects where the client can't agree on the entire scope of the project up front.

Each chunk of work in an Agile project is broken into smaller components called user stories. User stories represent specific features or functionality required by the customer. Agile teams review and prioritize these functions and features. These tasks are then delivered in short iterations called sprints, which typically last from one to four weeks. A sprint typically involves a number of user stories being developed and completed at the same time. A meeting to discuss the user stories and divide the work is called a scrum meeting.

In Agile project management, there are several frameworks to support the iterative and collaborative approach central to this methodology, including scrum, Kanban, and extreme programming.

A **scrum** is an Agile framework that focuses on delivering value through small, cross-functional teams working in sprints, and the product backlog contains a prioritized list of user stories or features. [0]Prior to the start of the sprint session, items from the backlog to be completed are planned out and chosen by team members. During each sprint, the team members select items from the backlog to complete. Scrum meetings, often referred to as stand-up meetings, backlog refinement, sprint planning, sprint review, and retrospective sessions, usually happen daily, which enables the team to adapt and improve continuously. The leader of the scrum meeting is called the **scrum master** and usually has a certification from PMI or other certifying bodies.

An Agile framework that helps managers visualize and optimize the flow of work. **Kanban** is a visual representation of tasks and how they flow through the project (Figure 9.7). A Kanban board typically consists of columns representing different stages of work, such as to do, in progress, or done. Each work item is represented by a card, and team members move the cards across the board as work progresses. As work is completed, team members start on the next task. The cards can be set up on a digital Kanban board (via tools such as Asana, Jira, or Smartsheet) or simply with sticky notes on a wall or whiteboard. The Kanban framework emphasizes limiting work in progress to maintain a smooth workflow while maintaining a continuous delivery schedule. This framework helps teams identify bottlenecks, optimize their processes, and respond quickly to changing priorities.

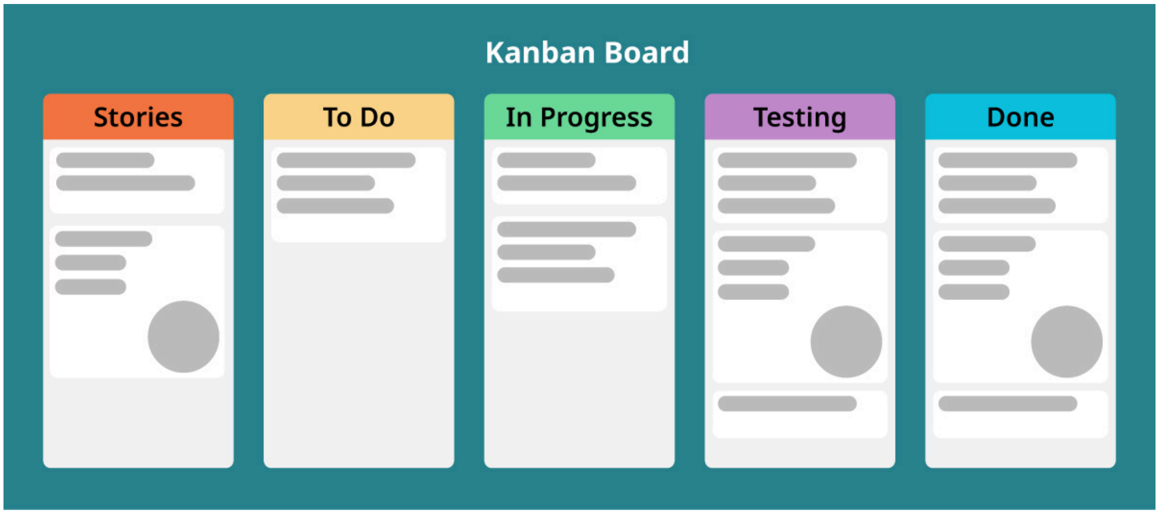


Figure 9.7 Referred to as a Kanban board, this type of Agile framework identifies the position of each component of work as the project progresses. (credit: modification of work "Abstract Kanban Board" by Jennifer Falco/Wikimedia Commons, CC BY 4.0)

Primarily used in the software engineering industry, **extreme programming (XP)** is an Agile methodology that emphasizes the use of software engineering practices to improve quality and responsiveness. Extreme programming also emphasizes customer involvement, short development cycles, and continuous integration and deployment. It incorporates practices like pair programming, test-driven development, frequent releases, and collective code ownership. By prioritizing customer value, XP teams can respond effectively to changing requirements and deliver high-quality software.

The advantage of an Agile approach is that it allows for flexibility and adaptability throughout a project's term, as teams can adjust their plans and incorporate feedback at the end of each sprint. The disadvantages are that the client must be willing to put in significant time since Agile requires many reviews and evaluations of work as the work continues. Many clients or companies do not have the time for their employees to be dedicated to a project in this manner. Overall, the Agile methodology works well for small- to medium-sized projects and in certain industries where flexibility and adaptability are crucial. For example, it might be suitable for a project that is highly regulated where standards may change frequently while you are building the deliverables, such as hospital information systems, or a new technology such as an AI application system where the capabilities grow daily.

PRINCE2 Methodology

PRINCE2 (Projects in Controlled Environments) is a project management methodology and certification that is widely recognized around the world. PRINCE2, much like PMBOK, uses a structured, process-based approach to managing projects, but it is designed to be scalable and adaptable, making it suitable for projects of various sizes and complexities. The PRINCE2 certification is often sought after by project managers, team members, and individuals involved in project management roles around the world because it provides individuals with a robust framework and a common language for managing projects effectively, as well as ensuring consistency and the use of best practices in project management processes. PRINCE2 is built on seven principles that guide its project management practices (Figure 9.8).

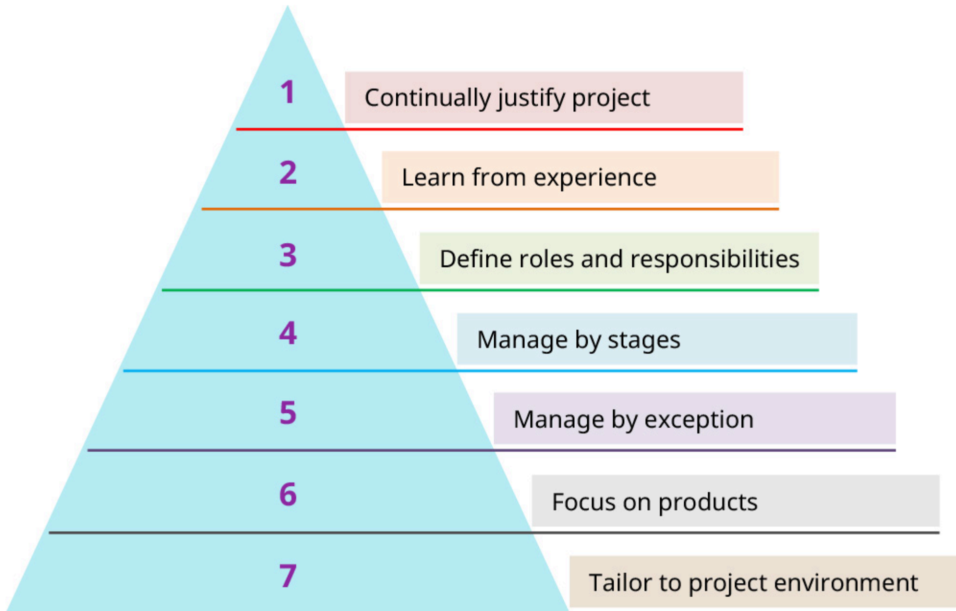


Figure 9.8 The PRINCE2 methodology is composed of seven guiding principles of project management. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Principle One: Continually Justify Project

A PRINCE2 project must have a reason to be started, and that reason must make sense from a business point of view; therefore, business justification is essential. The reason for the project, the funding and resources needed, and the predicted return on investment (ROI) must all be identified. If the ROI is greater than the cost of the project, then the project should be initiated. Each company typically has its own method of determining a minimum ROI threshold before a project is started. In some cases, due to regulations or changing technologies, companies must invest in projects to remain compliant with laws or stay competitive, which should be taken into consideration. The business justification should be revisited throughout the project to ensure that the ROI and reason for the project remain aligned or, at very least, the ROI does not drop below expected levels.

Principle Two: Learn from Experience

This principle involves collecting data on lessons learned from previous projects to avoid repeating risky and costly mistakes. In PRINCE2, project teams are constantly looking at the outcomes of the project to assess how well it is progressing and to determine whether any lessons learned can be identified and used immediately as the project continues. Each project can be unique and have its own set of challenges. These challenges can create risks or unknowns. Project teams need to understand the nature of change and risk and adapt to new situations. One example of learning from experience is discussing with other project managers with different experiences how they might respond to the challenge you are facing.

Principle Three: Define Roles and Responsibilities

Determining the roles and responsibilities of stakeholders in a project is critical. In PRINCE2 methodology, there is a process for identifying stakeholders that involves sorting them into three categories:

- Business sponsors: Stakeholders who make sure the project delivers value for money.
- Users: Stakeholders who are usually the people who will use the products once they have been created. They benefit from completion of the project.
- Suppliers: Stakeholders who provide the resources and expertise needed by the project to produce the products.

Not all companies or organizations have a dedicated team of project managers and other employees focused just on delivering projects. Project teams can be made up of people from various departments and companies, and therefore, defining each team member's roles and responsibilities with respect to the project is key to running it successfully and smoothly.

Principle Four: Manage by Stages

Like Agile project management, the PRINCE2 methodology aims to manage a project—and keep the project team flexible and responsive—by breaking the project up into chunks or smaller tasks that it refers to as stages. The three stages in PRINCE2 are planning, monitoring, and controlling, and they take place sequentially one stage at a time. The stages are separated by decision points, sometimes called control points. The need for continuous monitoring of the ROI is one of the reasons there are stages in PRINCE2. At the end of each stage, the team conducts a performance assessment of the last stage to decide whether the project should continue and, if it does continue, to determine any adjustments that need to be made.

This is also a point at which lessons learned can be assessed and applied for the next stage of the project. Like in the Agile methodology where there are points along the way when customer or client feedback is called for, the decision points of PRINCE2 function similarly, but the feedback comes from both the customer and other stakeholders in the company and focuses not only on the product deliverables but also on the performance and processes of the project team.

Principle Five: Manage by Exception

When managing by exception, the project manager has some leeway in the oversight of tasks, such as the schedule, scope, and costs, defined in accordance with company policy. In PRINCE2, the leeway is referred to as the tolerance level, or the extent to which project managers can accept the risk or need to escalate it. Project managers know that if an issue in the project passes a certain tolerance level, they must escalate it. If the project stays within the acceptable tolerance levels, the project manager can make adjustments where needed to keep the project on budget, within scope, and on time. In PRINCE2, managing by exception means that each level of leadership in the project manages the tolerance level below it in the organizational structure. So, if there is a major issue with a project, you may hear a project manager say the risk is outside the tolerance level range, meaning the issue needs to be escalated to the next level in the organizational chain of command.

There are six areas where tolerances or escalation points are applied: time, cost, quality, scope, risk, and benefit. This means the project manager must know the tolerance level for each of these areas and escalate an issue to the next level when necessary. For example, imagine your grandparents give you $500 on a credit card for transportation and dining out for the semester, with the instruction to let them know if the dollar amount gets too low or if you overspend by $20. This puts guidelines on the money but also ensures that the student does not have to get approval for every charge made that semester.

Principle Six: Focus on Products

Focusing on the product, its definition, and its requirements is important with PRINCE2. Project stakeholders join a project team bringing their own experiences and perspectives of the world, the project, and the product. Focusing on the details of the product is important to ensure there are no misunderstandings that waste time and money. To avoid this issue, the PRINCE2 methodology recommends developing a detailed product description that guides the project, manages expectations, and ensures the required deliverables. The product description should include a well-defined product purpose, composition, derivation, format, quality criteria, and quality process. It also determines a project's resource requirements, dependencies, and activities.

Principle Seven: Tailor to Project Environment

The principle of tailoring to the project environment is specific to the PRINCE2 methodology. A project should be tailored to suit the project's size, environment, complexity, capability, and risk. Similar to an Agile project being flexible and adaptable to the project needs, this principle means that managing really small projects does not require the full-blown documentation and requirements that more complex projects require. Some core principles must be followed to get the project delivered, but in PRINCE2, you should be cognizant of the environment in which the project should be managed. For example, if the environment of the company is one in which management is not focused on following every principle in the PRINCE2 methodology, then as the project manager, you should adapt to the environment and still deliver a quality product, on time, within budget, in scope, with minimal risks.

Tools of the Trade

There are several project management software tools that help project managers control the scope, schedule, and budget of a project. These tools can be as simple as using a spreadsheet to track deliverables and important milestones to expensive software designed specifically to manage large and complex projects. The size and complexity of the project would inform the decision as to which product to use.

Small projects can easily be managed using a spreadsheet like Microsoft Excel or Google Sheets. These products have add-ons and functions that can be programmed into a spreadsheet to deliver a schedule or a budget. Project managers can even create a dashboard and alerts within spreadsheets to help them stay on top of the critical aspects of a project.

Midsize projects might require more robust software tools such as Microsoft Project, Jira, and Asana. These tools feature items like Gantt charts, resource lists, and project budgets that are linked to a larger strategic budget or accounting system. They can also include several reporting features to allow the project manager to monitor schedule, costs, and scope, as well as robust graphics and color-coded systems to allow users to understand when something needs attention or when something is behind schedule. Artificial intelligence can be used to assist project managers in developing reports, monitoring schedules and budgets, and developing alerts to let project managers know when any of these components go beyond the escalation point.

Larger complex projects, such as those found in the construction industry and occasionally in IT, may require an even more robust system that can be customized to the type of project and have the company's strategic approach designed into the system, so that all users are using the same approaches and constraints. These complex systems also incorporate risks into their approach and provide various "what if" scenarios to help project managers compile the risks and constraints that may be part of a project. In addition, such systems serve as a knowledge base as they can store all the documentation and historical data associated with various projects. This assists with estimating pricing as well as developing future projects.

LINK TO LEARNING

Check out this list of top project management software tools (https://openstax.org/r/109SoftwareTool) that provides evaluations of products and the pros and cons for different types of projects.

Project Management Office

The **project management office (PMO)** is the department within an organization that provides the standards and guidelines to project managers for projects and governs how projects are initiated, planned, organized, implemented, managed, and closed. This group of individuals sits at the top of the entire project/program/portfolio management function. The PMO is equivalent to the C-suite of a company. Many times, project managers will be part of this department but not always. Some project managers may be serving as functional project managers while still residing in the department where they specialize. For example, an IS project manager may be part of the business side of the organization rather than in the PMO office or the IT department. The IS project manager might reside in the analytics, marketing, or operations departments.

The PMO, along with other members of the organization's leadership, might determine parameters like the structure of a project, who is able to manage such a project, the amount of risk the organization is willing to accept, and the escalation points for larger changes, issues, and risks. Additionally, the PMO might support project managers in various departments and make business decisions that the project manager cannot make to align the project with the organization. The PMO is also usually where project information and its historical data are kept. Any lessons learned from both successful and unsuccessful projects would be evaluated and policies would be put in place to facilitate a smooth project management process. Some organizations may not have a PMO but may still have units within the organization that govern and act like a PMO. In most organizations with a PMO, the primary functions of this group are as follows:

- Manage shared resources across all projects.
- Identify and develop project methodology, best practices, and standards.
- Coach, mentor, and train project managers.
- Monitor compliance with standards, policies, and templates, especially in highly regulated industries.
- Develop and manage policies, procedures, and other shared documentation.
- Coordinate communication across various projects.

Project management offices can take many different shapes and sizes, but the principles by which they operate remain the same (Figure 9.9).

Full Service	Shared Services	IT Development	Enterprise-level	Decentralized
Full PM governance	As-needed services for business units	Centralized portfolio oversight	Tied to overall leadership and financial strategy	Supportive, adaptive, and innovative

Figure 9.9 Project management offices can take different shapes, sizes, and roles, depending on what is needed for a project. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Some examples of the types and functions of common PMOs are as follows:

- Full service PMOs: They provide project management governance and guidance on how projects are delivered. They provide everything from policies, standards, best practices, approaches, and guidelines, to tools that project managers use.
- Shared services PMOs: They offer services as needed for things such as planning activities, risk management, performance tracking, and any other support the project manager may need. This type of PMO usually exists in an organization where there are independent business units.
- Information technology development PMOs: They oversee a portfolio, which is a collection of programs or groups of projects. These PMOs usually maintain oversight of all projects that require organizational approval and financial allocation. This type of PMO is centralized.
- Enterprise-level PMOs: They link the implementation of an organization's strategy with a portfolio of projects. This kind of PMO is established and tightly connected to the organization's leadership and overall strategy, and it usually operates within organizations that develop new products or have different business units or even different entities engaged in the development of many products.
- Decentralized PMOs: They usually implement innovative approaches in project management, such as the adaptive approach or Agile. This PMO plays more of a supporting role rather than serving an oversight function. The PMO takes a coaching approach to supporting project managers and business units and encourages training to make business owners and sponsors more effective at their jobs.

Program and Portfolio Management

Program and portfolio management are also part of an organization's structure and dependent on the capabilities of the business and its organizational strategy (Figure 9.10). A group of related projects, subprograms, and program activities managed in a coordinated way to obtain value of delivery is known as program management. Program management is above project management because program management encompasses several projects and is part of the bigger, overall portfolio for an organization. In the context of project management, portfolio management refers to projects, programs, and subportfolios, and operations managed as a group to achieve strategic objectives or value for the organization. For example, you may have an IT portfolio where you are delivering several projects related to an enterprise resource planning (ERP) system. The ERP system has several different projects related to the various parts of the project, such as human resources functions and accounts payable and receivable. You might have different project managers working on the implementation of each function of the ERP system because it is a large undertaking. Each of the project managers may report to the program manager of the ERP system or product. Above that, you might have clients you are implementing this ERP product for, and each of those projects reports up to a portfolio manager who may be a vice president or executive with the company.

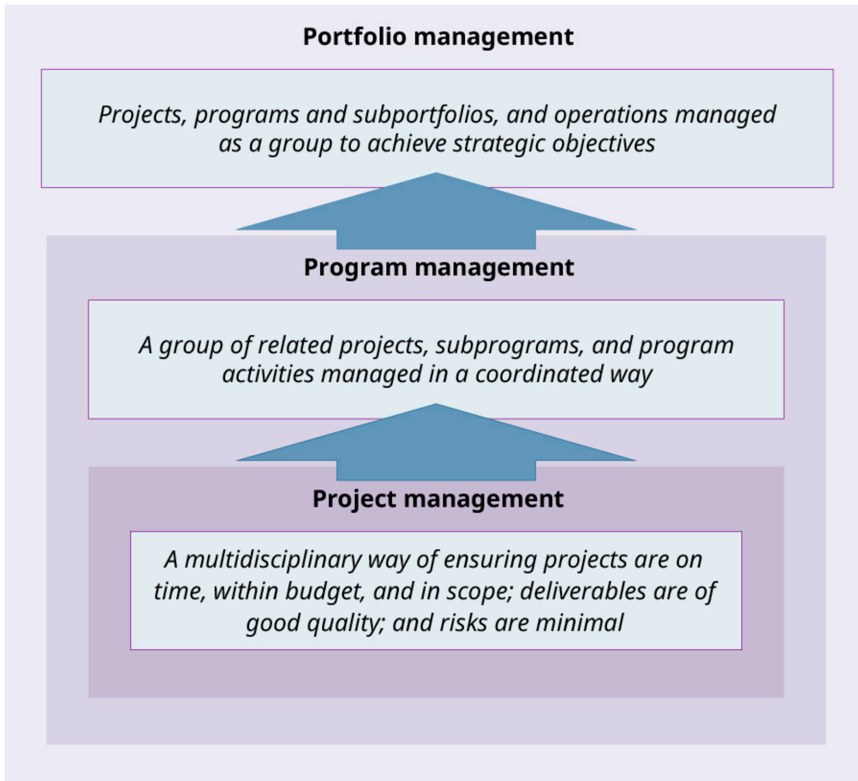


Figure 9.10 Project, program, and portfolio management are tied to one another in a hierarchical way, with programs encompassing multiple projects and portfolios encompassing programs and projects. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The purpose of program and portfolio management is to consistently deliver products and services that produce better results and sustainability for the organization and its projects. The goals of portfolio, program, and project management are to deliver value. Value is what keeps an organization in business and gives it a competitive advantage. This is why program and portfolio management are so important to the strategic operations of an organization.

Applying Project Management, Program Management, and Portfolio Management Skills

Now, let's consider a problem and determine which development approach—predictive, adaptive, or incremental—should be used. Pay particular attention to performance domains.

Case Study: Choosing a Project Management Approach

Pharrell is a consultant for a small financial company that has asked him to manage its ERP system project. An ERP system has functions for payroll, human resources, accounting, and finance. The company provides financial planning and advice to small business owners who need to set up 401(k) retirement accounts for their employees. The company's ERP system needs to meet all federal and state regulations for institutions that handle financial transactions. These regulations are monitored and controlled by the State Department of Labor and several financial regulatory bodies. The ERP system must take into account that the company must ensure that its employees are not making fraudulent financial transactions on behalf of their clients nor violating any insider trading or financial regulations when they offer advice on the retirement accounts to the small businesses.

The company is set up in a very flat organizational structure—meaning there are three vice presidents (one each for accounting and finance, operations, and sales) and a president who oversees all three vice presidents. There are several managers and supervisors in the company as well as administrative and operational employees who report to the three vice presidents. The company has just hired ten new staff to make a total of fifty-nine employees that work directly for the company. Some of the employees working on client accounts have legal backgrounds. The ERP is a big system for the company. It has chosen to implement such a large system because it wants to double its clients in the next two years, and this would mean hiring more employees.

The company expects Pharrell to manage and implement the new ERP system without a lot of input from the internal company employees, except for the three vice presidents and the president. Only the leadership of the company will participate in the project, but all employees are stakeholders. The company will make employees available to test the system, but Pharrell is expected to provide all the other human resources needed for the project. Since he has implemented ERP systems before, he already has several individuals to work on this project and is confident he can do the work.

Selecting a Project Development Approach

Recall what you learned about predictive, adaptive, and incremental project development. Consider the pros and cons of each within the specifics of this project:

- Degree of innovation: This project probably doesn't require innovative thinking to solve a problem. According to Pharrell, he has a team that has worked together before; therefore, they do not need to consider assembling a team with innovative thinkers or use this approach.
- Requirements certainty: The requirements for the system should be spelled out well since this is an implementation of an ERP system, and there is only so much that needs to be modified to meet the company's requirements. So, a predictive approach may be the way to go.
- Scope stability: The scope of the deliverables will probably not change given that this is an off-the-shelf ERP system, but since the actual end-user stakeholders aren't involved, the scope may change, especially since the users are going to test the system. A predictive approach would be needed if the scope were stable.
- Ease of change: This also deals with scope and stability. If the deliverables are not going to change much, then a predictive approach should be used.
- Delivery options: Because an ERP system has many different functions, the project could be broken down into functions and different groups could work on each function that needs to be delivered; an incremental or iterative approach could be used.
- Risk: One risk for the project would be that the deliverables may change once the end users are utilizing the system, or the vice presidents may not have the time to dedicate to the project to determine the requirements. For a project with these kinds of risks, a predictive approach would work best, at least in the beginning, as it would help define the requirements.
- Safety requirements: The product should not have any safety-related requirements that would physically harm someone, so this consideration may not apply to the project.
- Regulations: This project would be highly regulated since the nature of the company is in finance and retirement accounts. Even though the business of the company may not have a lot to do with the ERP system, other than accounts receivable, the project does have to implement some of the regulations required to manage the employees of the company.

Based on this analysis of the various approaches, this project should be developed using the predictive approach. With the number of regulations to satisfy and the fact that the scope will probably not change much because of these regulations, this approach will serve Pharrell well. This doesn't mean that later in the project an incremental or Agile-related approach would not be more useful, it just means that up front, the more planning Pharrell can put into this project, the better the project will be executed, and the greater chance that the delivery will be smooth.

9.2 Setting Up and Managing Projects for Success

Learning Objectives

By the end of this section, you will be able to:

- Explain the stages of a project from initiation to closing
- Explain how to develop a project plan and schedule
- Determine how to identify, evaluate, and mitigate project risks

Project management is about properly understanding the requirements for a project and being able to manage that project based on scope, costs, schedule, quality, and risks. Project managers need to understand the role each of these plays on the project from initiation to closing. The PMBOK approach provides guidance on how to set up and manage projects successfully.

Project Stages

In project management, the successful execution of a project depends on a structured approach applied across various stages. These stages provide a framework for managing projects from their inception to their completion. Typically, there are five stages of a project, and various tasks within each stage make up the project management framework (Figure 9.11). The five stages are as follows:

1. project initiation
2. project planning
3. project execution
4. monitoring and control
5. project closure

Figure 9.11 A PMBOK approach shows the five main stages of project management linearly. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The PMBOK defines a comprehensive set of processes that guide project managers through each stage of a project. Following the processes ensures the project will be on time, be within scope and budget, have minimal risk, and be of acceptable quality.

Project Initiation

The **project initiation** stage marks the creation of a project and involves defining its purpose, objectives, and stakeholders. It's like creating a road map for a project journey. Most times, projects come from the top down or bottom up—meaning that they are sometimes initiated by the company's leadership and sometimes by managers within the company. The third way a project can be initiated is through a client. For example, your company may be selling a complex software application that requires the product to be carefully customized to a client's operations. This would require a project to be initiated for the purpose of a sale made to a client. There are many factors that go into how an organization initiates projects and decides how they will be managed. During the initiation stage, project managers undertake several key activities.

Project Identification and Selection

Project identification entails recognizing opportunities or challenges that warrant a project's initiation. Projects may be initiated to address market demands, meet organizational goals, or tackle specific problems. Once identified, potential projects undergo an evaluation based on factors such as strategic alignment, feasibility, and resource availability. Best practices suggest using methods like cost-benefit analysis, SWOT (strengths, weaknesses, opportunities, and threats) analysis, or business case development to assess project viability.

Stakeholder Analysis

Understanding stakeholders and their influence is crucial for project success. It is important to understand that failure to properly identify a key stakeholder can jeopardize an entire project. Project managers employ techniques like stakeholder mapping and analysis to identify key stakeholders, assess their expectations, and determine their level of involvement. Stakeholder engagement strategies are formulated to foster effective communication, collaboration, and stakeholder satisfaction throughout the project life cycle (PLC).

Project Charter Development

The **project charter** serves as a formal document that authorizes project initiation. Many large organizations may have a committee or leaders that determine which projects will be authorized to begin the charter initiation process. The project charter outlines the project's objectives, scope, constraints, and success criteria. It also establishes your authority as the project manager and provides a high-level view of the risks and stakeholders involved. Developing a comprehensive project charter establishes a clear direction for the project and sets the stage for subsequent project planning activities.

Project Planning

Once your project has kicked off, it's time to dive into creating a project management plan to ensure project success. This stage is about defining the project's scope and the details of how progress will be accomplished. It is important to note that the scope, schedule, risks, and budget are all part of this stage and set the parameters for a successful project. A scope document, RACI documents, and project plan for how the project will be managed should all be considered during this stage.

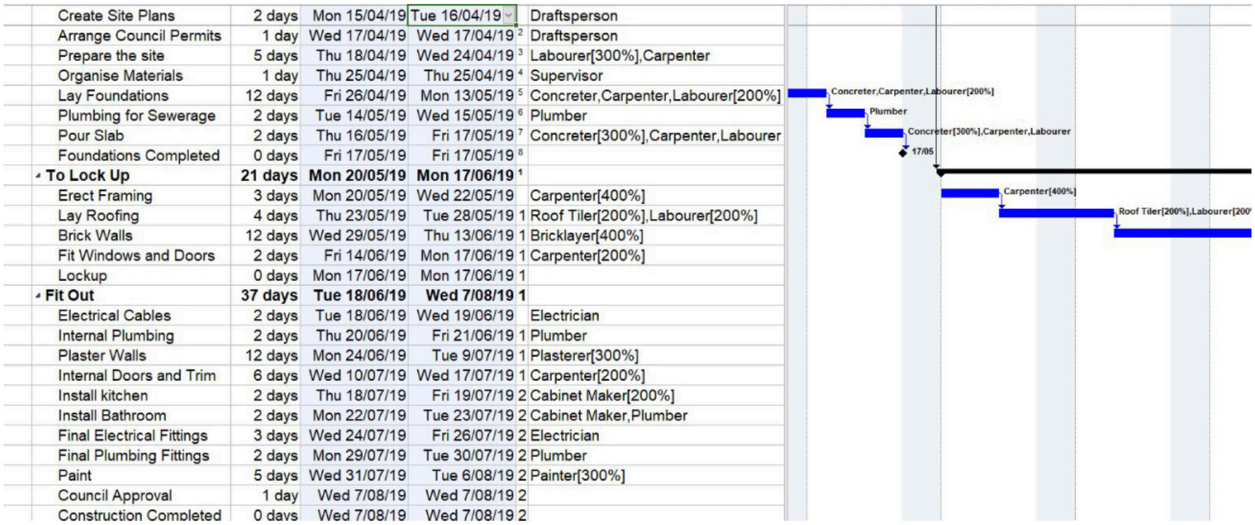
Scope Definition

The **scope** includes the deliverables, objectives, and requirements of the project. Defining scope is like drawing the boundaries of your project. You want to be very clear about what's included and what's not. To establish a clear understanding of what the project entails, project managers employ a **statement of work**, a document detailing the requirements, deliverables, schedule, and responsibilities of the stakeholders of a project. Scope verification and control processes are also put in place to manage changes and ensure alignment with stakeholder expectations. Control processes mean setting up a change management process to keep track of the scope and the budget for these changes.

As a project manager, one of your most important jobs is to minimize **scope creep**, which is where the scope of the project grows beyond what was agreed on in the planning stage of the project as requirements are changed or modified down the line. It is a good idea to set up processes to help manage the scope, such as getting sign-off on a scope document before the project begins and setting up a proper procedure for stakeholders to change or modify the scope, called a **change management process**.

Schedule Development

Developing an accurate project schedule involves sequencing project activities, estimating durations, and creating a timeline (Figure 9.12). Techniques like network diagrams, critical path analysis, and schedule compression aid in scheduling activities and identifying dependencies. Project managers use scheduling tools and software to optimize resource utilization, manage project constraints, and mitigate schedule risks.



Create Site Plans	2 days	Mon 15/04/19	Tue 16/04/19		Draftsperson
Arrange Council Permits	1 day	Wed 17/04/19	Wed 17/04/19	2	Draftsperson
Prepare the site	5 days	Thu 18/04/19	Wed 24/04/19	3	Labourer[300%],Carpenter
Organise Materials	1 day	Thu 25/04/19	Thu 25/04/19	4	Supervisor
Lay Foundations	12 days	Fri 26/04/19	Mon 13/05/19	5	Concreter,Carpenter,Labourer[200%]
Plumbing for Sewerage	2 days	Tue 14/05/19	Wed 15/05/19	6	Plumber
Pour Slab	2 days	Thu 16/05/19	Fri 17/05/19	7	Concreter[300%],Carpenter,Labourer
Foundations Completed	0 days	Fri 17/05/19	Fri 17/05/19	8	
To Lock Up	**21 days**	**Mon 20/05/19**	**Mon 17/06/19**	**1**	
Erect Framing	3 days	Mon 20/05/19	Wed 22/05/19		Carpenter[400%]
Lay Roofing	4 days	Thu 23/05/19	Tue 28/05/19	1	Roof Tiler[200%],Labourer[200%]
Brick Walls	12 days	Wed 29/05/19	Thu 13/06/19	1	Bricklayer[400%]
Fit Windows and Doors	2 days	Fri 14/06/19	Mon 17/06/19	1	Carpenter[200%]
Lockup	0 days	Mon 17/06/19	Mon 17/06/19	1	
Fit Out	**37 days**	**Tue 18/06/19**	**Wed 7/08/19**	**1**	
Electrical Cables	2 days	Tue 18/06/19	Wed 19/06/19		Electrician
Internal Plumbing	2 days	Thu 20/06/19	Fri 21/06/19	1	Plumber
Plaster Walls	12 days	Mon 24/06/19	Tue 9/07/19	1	Plasterer[300%]
Internal Doors and Trim	6 days	Wed 10/07/19	Wed 17/07/19	1	Carpenter[200%]
Install kitchen	2 days	Thu 18/07/19	Fri 19/07/19	2	Cabinet Maker[200%]
Install Bathroom	2 days	Mon 22/07/19	Tue 23/07/19	2	Cabinet Maker,Plumber
Final Electrical Fittings	3 days	Wed 24/07/19	Fri 26/07/19	2	Electrician
Final Plumbing Fittings	2 days	Mon 29/07/19	Tue 30/07/19	2	Plumber
Paint	5 days	Wed 31/07/19	Tue 6/08/19	2	Painter[300%]
Council Approval	1 day	Wed 7/08/19	Wed 7/08/19	2	
Construction Completed	0 days	Wed 7/08/19	Wed 7/08/19	2	

Figure 9.12 Scheduling tools enable project managers and team members to visualize an entire project and understand how each step in the project coordinates to meet project deadlines, as in this example from a construction project. (credit: "Tasks" by Christine Nicholas/Flickr, CC BY 2.0)

Resource Planning

The task of determining what resources are needed and when they will be needed is called **resource planning**. Project managers assess the availability and capabilities of resources, both human and nonhuman, to ensure efficient resource utilization. By considering factors such as resource skill sets, costs, and constraints, project managers develop resource management plans that align with project objectives.

Budgeting and Cost Management

Effective cost management ensures that projects stay within budget constraints. Project managers estimate costs, create budgets, and monitor expenditures against actual project costs. Techniques such as cost estimation, cost aggregation, and earned value management aid in budget development and cost control.

The planning stage is a perfect point in the project to ensure that you understand the PMO's or the company's escalation policies. Project managers use the PMO or company policies to decide when to escalate project overruns that can negatively impact the project. An **escalation policy** determines when the project manager should report budget issues, such as being under or over budget. Some projects may have specifications dictating that when projects are under budget, the client receives the excess portion to make additional changes later in the project or receives that money back on future payments. Think of a project like going on a weekend trip where your parent gives you a set amount of money to spend on the trip. They may say you can spend up to that amount, but if you don't spend it all, you can't keep the change, and if you go over that amount, it comes out of your pocket. This is why project managers need to be good at budgeting and managing costs on projects. Knowing the company's policies and the client's requirements is key to successfully managing budget and costs.

Project Execution

With a plan in place, it's time to execute. This is where all the action happens. The project manager monitors progress, addresses issues as they arise, and ensures the project stays on track. The **project execution** stage involves implementing the project plan, managing resources, and monitoring progress. This stage focuses on coordinated effort and effective communication. This might be the shortest phase as far as the number of tasks to complete, but the work has just begun. The project manager goes from planning to executing the plans, which include a lot of other human beings and resources that need to be monitored.

During project execution, project managers oversee the execution of planned activities, ensuring that work is performed in accordance with the project plan. This includes coordinating resources, managing risks, resolving issues, and ensuring quality control. Effective leadership and stakeholder engagement are critical in fostering collaboration and maintaining project momentum. This is the stage at which communication becomes critical. You might have leaders and supervisors who have never worked together before or never worked with you. Set expectations and make sure everyone knows their job for the project.

Monitoring and Control

Continuous monitoring and control are vital to tracking project performance and ensuring adherence to the project plan, all in service to ensuring a successful end project. Project managers employ techniques such as progress tracking, performance measurements, and variance analysis to assess project status. Key performance indicators are established to monitor project objectives, deliverables, and milestones. Timely identification of deviations enables project managers to take corrective actions, adjust plans, and manage project changes.

The project manager may take on several different roles during this stage. They are leaders, managers, accountants, and human resources experts; they may also be technical experts depending on their backgrounds. Project managers must anticipate, imagine, adjust, fix, and stay on top of everything related to their project. If a project manager has a good team to work with, this part can be easy, but if the project manager's team develops conflicts, this could mean a delay in deliverables or failure to deliver the right product or service.

Part of monitoring and control and the planning stages is risk management. Identifying, analyzing, and responding to risks is crucial to project success; thus, risk management is one of the most important jobs of the project manager. The process of **risk management** encompasses risk identification, qualitative and quantitative analysis, risk response planning, and risk monitoring and control. By actively managing risks throughout the PLC, project managers enhance project resilience and minimize negative impacts.

Project Closure

The **project closure** stage brings the project to a formal conclusion, ensuring that all project objectives are met and deliverables are handed over. This is the stage at which team members return to their previous work, or they move on to the next project. This is not true for the project manager. The project manager must complete all the paperwork and ensure the client or customer is happy with the outcome of the project. Project managers will ensure they met the budget or even came in under budget numbers, and the timeline would be verified to ensure that the project was delivered within the timeline agreed on by the client.

Deliverable Acceptance

One of the important items on a project manager's closeout checklist should be the acceptance of deliverables. At this point in the process, project managers verify that the deliverables have been assessed and that all deliverables meet the scope and stakeholder requirements of the project. Formal acceptance procedures and sign-offs are obtained to confirm the satisfactory completion of deliverables. Best practices recommend involving stakeholders in the acceptance process to validate deliverable quality and promote customer satisfaction.

Project Evaluation: Knowledge Transfer and Documentation

Postproject evaluation assesses the project's overall performance, including its success in meeting objectives, adherence to schedule and budget, and stakeholder satisfaction. Evaluation findings contribute to organizational learning, enabling improvements in future project management processes and practices. As the project concludes, knowledge transfer takes place to capture lessons learned and share best practices. Documentation of project artifacts, reports, and records facilitates knowledge retention and supports future projects. Project managers conduct project reviews and retrospective meetings to analyze project performance, identify areas for improvement, and enhance organizational learning. Usually, the PMO or another project manager would conduct an audit of the project and survey stakeholders on how to improve projects in the future. This information is collected and utilized to help PMOs change processes or policies to operate more efficiently. Some organizations may not have one electronic area within which to keep all of their project data, so it is important the project manager takes time to organize the knowledge and safely keep the data where it can be accessed for the next projects.

Developing a Project Management Plan and Schedule

To ensure successful project execution, project managers should develop a comprehensive project plan and schedule using real requirements and documentation. This phase involves several key steps, each of which plays a significant role in shaping the project's direction and facilitating efficient execution.

Defining Project Objectives

The first thing the project manager must do is clearly articulate the project's objectives and desired outcomes. This involves engaging stakeholders and understanding their expectations for the project and the deliverables. It is essential to establish SMART (specific, measurable, achievable, relevant, and time-bound) objectives to provide a clear direction for the project. Without this step, you can get to the end of the project and find the client is unhappy.

Identifying Deliverables

The project manager must identify with the stakeholders, including the client, specific deliverables the project will produce, including reporting and any other updating the stakeholders need. These deliverables can be tangible products, services, or outcomes that contribute to the project's success. By identifying and defining deliverables, the project team gains a shared understanding of what needs to be accomplished.

Defining Scope

As you learned, the project scope defines the boundaries of the project, including what is included and what is excluded. A well-defined scope helps manage expectations, prevent scope creep, and ensure that the project remains focused on its intended outcomes. The project manager must also clearly document the project scope statement to provide a reference point throughout the project and ensure that the product and/or service being delivered meets stakeholder expectations as defined in the scope.

Work Breakdown Structure

A **work breakdown structure (WBS)** helps the project manager understand how the deliverables will be scheduled and any dependencies there might be in completing other deliverables, essentially breaking down the work into smaller, more manageable work packages and tasks. A WBS allows the project manager to see the project as bite-sized pieces and tackle them one by one. For example, if you have one team that needs to produce two deliverables, you may need to resource the first deliverable or divide the team if there are enough individuals to complete both deliverables on time. A WBS provides a structured view of the project's tasks, activities, and subactivities, using some of these techniques:

- Activity sequencing: A WBS can identify logical dependencies between project activities to determine which activities must be completed before others can begin and establish the sequence in which activities should be executed. Dependency relationships can be of various types, including finish-to-start, start-to-start, finish-to-finish, and start-to-finish. This step helps in determining the flow of tasks and understanding the project timeline.
- Estimating activity durations: Accurate duration estimates help in creating a realistic project schedule. To estimate the time required to complete each activity, the project manager must consider resource availability, complexity, and dependencies. The project manager can use historical data or expert judgment if they have the experience. There are several estimation techniques that would be taught in a project management course or training, such as analogous estimating, parametric estimating, and three-point estimating to determine activity durations.
- Resource planning: The project manager needs to identify the resources required to execute the project

activities as well as assess the availability and allocation of resources. This requires a solid estimation of the team's skills, expertise, and availability throughout the project. Resources could include human resources, equipment, materials, and any other necessary assets. Good resource planning ensures that the right resources are assigned to the right tasks at the right time.

Developing the Schedule

Using the activity durations, dependencies, and resource planning, the project manager can create a project schedule. The schedule outlines the start and end dates for each activity and provides a road map for project execution. The project manager also considers constraints, milestones, and critical path analysis to ensure that the schedule reflects realistic timelines and dependencies.

Monitoring and Control

When the project is ready to move along with its tasks, the project manager must establish processes and tools for monitoring the project's progress and managing any deviations from the planned schedule. The project manager must regularly track the actual progress against the planned schedule, identify variations, and take corrective actions as necessary, sometimes in a very short period of time. The project manager also needs to conduct regular project status meetings, update the project plan and schedule, and communicate changes to stakeholders. This is one of the busiest times for a project manager.

ETHICS IN IS

The Ethics Guy Podcast

Project managers need to make decisions on a regular basis that impact the project from an ethical perspective. This podcast episode specifically tackles project manager ethics (https://openstax.org/r/109PMEthics) and features Bruce Weinstein, "The Ethics Guy," discussing what a project manager should do and whom they should be. The podcast *Manage This* is directed at project managers as they make important decisions not just for projects, but also for organizations, which involve resources, budgets, and leadership skills.

The Plan and Schedule in Action

To illustrate the importance of project planning and scheduling, consider a scenario of developing a new software application. Imagine you are a project manager responsible for overseeing the software development life cycle, from inception to deployment, at a high-tech firm that sells IT services to small- and medium-sized organizations. Your organization has recognized the need for a customer relationship management (CRM) system to enhance customer interactions and streamline business processes.

To effectively support the sales and customer management processes of a medium-sized organization that sells search engine optimization (SEO) services to large organizations, the CRM system your organization needs encompasses a range of specific requirements. These requirements are tailored to the organization's unique needs and the nature of the services it provides, such as reviewing SEO data to determine gaps in web strategy.

The first thing you must do is accurately identify stakeholders in the project to ensure they are represented in the requirements gathering process. Once the stakeholders are identified, you can set up the processes for how to gather the needs and wants of the team and the organization. For example, should you have one big meeting, or should you break down various groups by function and meet with them separately? Or should you select certain individuals to be part of one higher-level meeting and then have others be part of another broad meeting to gather requirements?

As a project manager, the hardest part of the requirements gathering process is determining the difference between a “must-have” (needed) feature or function and one that is “nice to have” (wanted). Identifying both the needs and wants in the requirements is necessary when budgeting and designing the solution. If there is money left in the budget, you may be able to deliver on some of the wants instead of just the must-have features and functionality.

Table 9.1 outlines the key requirements for the CRM system gathered through stakeholder meetings and analysis of the future needs of the organization for this scenario.

Requirements Document for XYZ Corporation
Through meetings with key stakeholders and end users, the following areas have been defined as departments or functions that will utilize the CRM:
Lead management: • Capture and track leads generated through various marketing channels (e.g., website, social media, email campaigns). • Assign leads to sales representatives based on predefined criteria and territories. • Monitor lead progression through the sales pipeline and track relevant interactions and activities. • Provide automated lead nurturing capabilities to engage and convert potential customers.
Contact and account management: • Maintain a centralized and up-to-date database of contacts and accounts, including key stakeholders within customer organizations. • Capture contact details, job titles, contact history, and any relevant notes or preferences. • Enable easy segmentation and categorization of contacts based on various criteria (e.g., industry, organization size, revenue).
Opportunity and sales management: • Manage sales opportunities and track their progress through the sales cycle. • Record and update opportunity details, including deal value, estimated close dates, and associated activities. • Generate sales forecasts and reports to analyze sales performance and pipeline.
Service management: • Support the management of SEO service delivery, including project tracking, task assignment, and progress monitoring. • Enable collaboration among sales, service delivery teams, and clients to ensure smooth execution and customer satisfaction. • Record and track service-related interactions, requests, and issues.
Communication and collaboration: • Facilitate seamless communication and collaboration among sales representatives, account managers, and clients. • Enable email integration to capture and log email communications within the CRM system. • Provide a centralized platform for internal collaboration and knowledge sharing related to customer accounts and opportunities.

Table 9.1 Sample Requirements Documentation A requirements document for selling SEO services might begin with something like this example.

Requirements Document for XYZ Corporation
Reporting and analytics: • Generate customizable reports and dashboards to monitor key sales metrics, performance, and trends. • Provide real-time visibility into sales pipeline, revenue forecasts, and customer engagement. • Support data-driven decision-making through advanced analytics and visualization capabilities.
Integration and scalability: • Integrate with other relevant systems such as marketing automation, project management, and invoicing. • Allow customization and scalability to accommodate future growth and evolving business needs. • Ensure data integrity and consistency across integrated systems.

Table 9.1 Sample Requirements Documentation A requirements document for selling SEO services might begin with something like this example.

These requirements will be documented in the requirements document that eventually will become the scope of the project. Project managers need to have this requirements document to determine the solution, budget, and timeline for the project.

Developing a well-structured project plan and schedule is critical to ensure a successful CRM software implementation. The project plan outlines the entire scope of work, including the specific deliverables, milestones, and activities required to complete the project. It serves as a road map, guiding the project team through the various phases of development, testing, and deployment.

Planning for the Solution

The next step in developing the project plan and schedule is to understand the solution or how the organization will go about finding the right solution. The solution can be developed in one of two ways: (1) use the requirements document to draft a request for proposal (RFP) to acquire vendors who can supply or build the solution or (2) determine the internal and external resources needed to build the solution and integrate it into the organization. Depending on the resources of the organization, it may be better to select a vendor who can deliver an off-the-shelf CRM system and integrate it with the internal organization. For the purposes of this scenario, a vendor will deliver the complete solution.

Project Objectives

In this case, the organization has defined the objectives to include improving customer satisfaction, increasing operational efficiency, and boosting sales revenue. These clearly defined objectives provide direction for the project and align the efforts of the project team with the organization’s strategic goals.

Deliverables

Since the organization is choosing an off-the-shelf solution and will have a vendor implement and integrate the CRM solution, the project manager’s deliverable is an RFP with the requirements categorized and defined, such as customer data management, sales pipeline tracking, and reporting functionalities. Under each of these categories, the actual requirements would be written to include in the RFP.

Next comes the selection process. The project manager will need to develop the criteria and process for the selection of the vendor. This information will become part of the RFP, so vendors know what to expect. For example, you may require the vendor to submit a proposal and a detailed demonstration of the features and functionalities requested in the requirements. Or you may require the vendor to submit their proposal in person as a presentation to key stakeholders.

Last, you will need to detail the transition and management plan for the project. This plan describes how the organization will work with the vendor and who the key points of contact would be. Typically this includes the project manager and, depending on the questions the vendor may have about the specifics of the project, perhaps someone from the organization's leadership team or technical department.

Scope

Once the objectives and deliverables are defined, the project manager proceeds with scoping the project. Determining the boundaries of the project involves establishing what is within the project's scope and what is not. Scoping this project should be simple since you are selecting a CRM vendor who will provide a solution and integrate it into your organization. As a member of the company acquiring the software, all you must manage is the RFP process and how you will work with the vendor to implement the solution. The vendor should provide its own project manager to work with you.

Creating a Work Breakdown Structure

With the scope defined, the project manager then creates a WBS (Figure 9.13). In the case of the CRM software development, the WBS could include activities such as requirements gathering, system design, coding, testing, user training, and deployment. The WBS breaks down what needs to be part of the schedule and estimates how long each task might take. Earlier the work was defined as follows:

- initiating the project
- acquiring the project requirements
- developing the RFP
- selecting the vendor
- overseeing the vendor's implementation, integration, and training services

First, organize these master tasks across the top of the WBS. Under each master task, break down the task into smaller tasks and organize those accordingly.

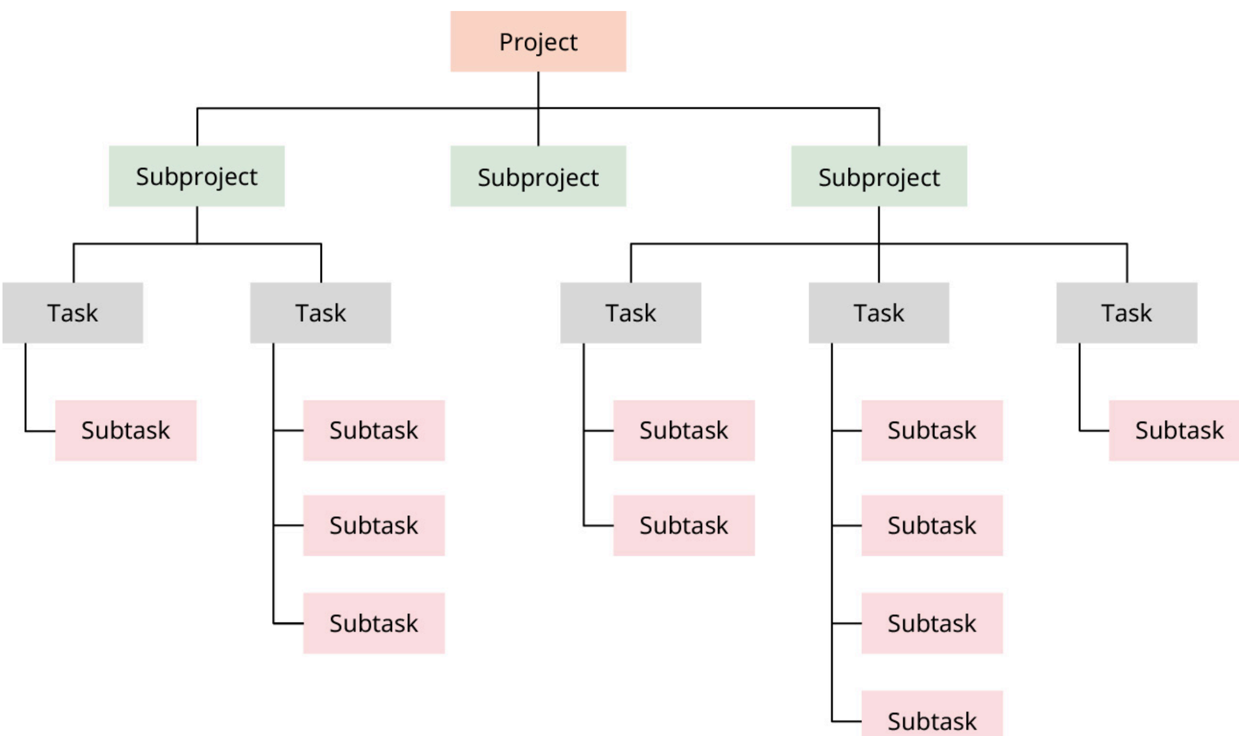


Figure 9.13 A work breakdown structure helps to organize, prioritize, and visualize what steps are needed to complete a project. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Sequencing

Once the WBS is established, the project manager can identify the dependencies between activities and establish the sequence in which they should be executed. Sequence these subtasks for each master task and assign the number of work hours it will take to complete each task. For instance, system design cannot begin until the requirement's gathering phase is completed. This activity sequencing ensures a logical flow of work and enables efficient resource allocation. Remember that your WBS will help you understand the dependencies of each task and the flow of the project and help determine the time each task will take to be completed.

To estimate the duration of each activity, consider various factors such as resource availability, complexity, and dependencies. For example, acquiring the project requirements may take a while because this task is dependent on the schedule of the stakeholders involved and the approval process required.

Next identify the resources required to carry out the project activities. This could include software developers, testers, and database administrators, as well as infrastructure resources for this project. Ensuring that the right resources are allocated to the right tasks at the right time is essential for maintaining project efficiency.

Bringing It All Together

Once the project plan is developed, the project manager will go to the calendar and begin using the WBS to turn the sequencing, resource allocations, and durations for each task into a project schedule. The schedule outlines the start and end dates for each activity, considering the estimated durations, dependencies, and resource availability. It provides a clear timeline for the project team and stakeholders, facilitating coordination and ensuring everyone is aware of key milestones and deadlines.

FUTURE TECHNOLOGY

Using Artificial Intelligence or GPT for Project Management

Both AI and GPT are big in the business industry. How can project managers use GPT to assist in their work activities? Well, let's ask Bing GPT, which was running on GPT Version 4 at the time this was written. In answer to this question, Bing GPT provided some very interesting information and an interesting recommendation.

> Hello, this is Bing. I'm glad you asked. AI or GPT can help with project management in many ways, such as:

- Creating project plans and timelines by providing information on your assignment and getting suggestions from ChatGPT, an AI tool that uses machine learning to generate natural language responses.
- Getting feedback or optimization tips on your existing project plans or timelines by asking ChatGPT questions and getting in-depth answers.
- Delegating tasks to your team members by providing ChatGPT with the scope of the project and the strengths and weaknesses of each team member, then asking who should take on which task.
- Boosting productivity and improving project workflows by using AI-powered solutions that can automate task creation, provide PM insights, and handle uncertainty and risk.

> However, there are also some limitations and challenges of using AI or GPT for project management, such as:

- Lack of context or expertise in certain areas or industries, which may lead to weak or inaccurate recommendations.
- Difficulty in dealing with complex or ambiguous situations that require human judgment or

creativity.
- Ethical or legal issues that may arise from using AI-generated content or data without proper attribution or consent.

It is important that, if used, AI or GPT serve as a supportive tool rather than a replacement for human project managers. You should always verify the quality and validity of any AI-generated content or data before using it for a project. You should also be aware of the ethical and legal implications of using AI or GPT for project management and follow the best practices and guidelines for responsible AI use.

Project Risks

Risk assessment and management are important in today's business world. In project management, effective risk assessment is crucial for managing successful project outcomes. Identifying, evaluating, and mitigating project risks are essential processes that help managers project, anticipate, and address potential obstacles that can impact project objectives.

Risk management is something people can use in every part of life, so the risk assessment described here can be applied to other activities, such as buying a car or getting a job, to determine what the impact of those risks would be on your life financially, time-wise, or in any other way.

Identifying Risks

The first step in a risk assessment is to define what a risk is and how it should be categorized. A **risk** is an event or condition that has a negative effect should it occur during a project. Identifying project risks involves systematically identifying potential events or circumstances that may have an adverse impact on project objectives. Project risks should be identified throughout the project and monitored for severity. Each time there is a delay in a deliverable, the chance of completing the project on time could become a risk or impact on the cost or budget of the project. There are various strategies for identifying risks in a project.

Engaging Stakeholders

Stakeholders possess valuable knowledge and perspectives on different aspects of the project that you may not have or that they are more familiar with. By involving stakeholders in risk identification activities, project managers can tap into their expertise and gain a comprehensive understanding of potential risks. Here are some tips on engaging stakeholders[1] :

- Brainstorming sessions: Organize brainstorming sessions with the project team, subject matter experts, and relevant stakeholders. It is the project manager's job to encourage participants to freely express their thoughts and ideas about potential risks. This collaborative approach fosters creativity and allows for the identification of risks from diverse viewpoints.
- Interviews and workshops: Conducting interviews or workshops with key stakeholders can elicit their insights on risks specific to their areas of expertise. These interactions provide an opportunity to explore risks associated with project requirements, technology, resources, and external factors.

Utilizing Risk Identification Techniques

In addition to stakeholder engagement, various techniques can be employed to systematically identify project risks[2] :

- Checklists: A favorite among project managers, checklists that cover a wide range of risk categories relevant to the project can serve as prompts to stimulate thinking and ensure comprehensive risk identification. Examples of checklists include industry-specific risk checklists, lessons learned from

1 Michael M. Bissonette, *Project Risk Management: A Practical Implementation Approach*. (Project Management Institute, 2016).
2 Michael M. Bissonette, *Project Risk Management: A Practical Implementation Approach*. (Project Management Institute, 2016).

previous projects, or risk categories derived from standards and best practices. The key is not to reinvent a process but to use the resources you already have available. The PMI provides several resources for risk assessment documents.

- Historical information review: Before you begin to gather risk data, analyze historical project data, lessons learned, and postmortem reports from previous projects to identify risks encountered in similar contexts. This technique leverages the experience and knowledge gained from past projects to proactively identify risks that may arise in the current project. Look for prior risk assessment documents from similar projects and determine if this project could encounter the same types of risks.
- Cause-and-effect analysis: Apply cause-and-effect analysis techniques, such as fishbone (Ishikawa) diagrams (Figure 9.14) or the five-whys technique, to identify potential risks by exploring the underlying causes. This technique helps uncover risks that may not be immediately apparent and enables a deeper understanding of their root causes.
- SWOT analysis: A SWOT analysis is used in business for determining new strategies and developing new products. The SWOT analysis identifies risks related to the project's internal and external environment and helps identify potential threats and weaknesses that may impact the project's success.
- Expert judgment: More experienced project managers have a lot of history with various types of projects and can readily identify risks. Junior project managers should seek input from subject matter experts or experienced professionals who possess domain-specific knowledge. Their expertise can help the project manager identify risks that may be unique to the project domain or require specialized insights.

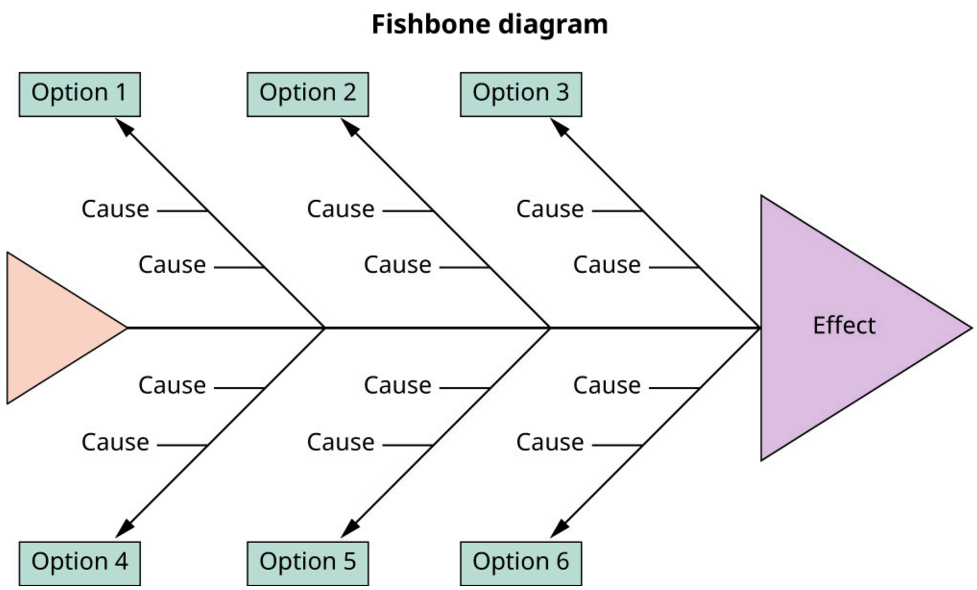


Figure 9.14 A fishbone diagram can help to analyze cause and effect of potential risks, helping the project manager to plan for adjustments needed to the project, schedule, or budget. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Evaluating Risks

Once risks are identified, they must be evaluated for their impact, probability, and severity related to the project. To evaluate risks of the project, conduct an overall risk assessment (Figure 9.15). The risk assessment provides the team with an overall level of risk or risk exposure number and takes into consideration any threats to the project, including its budget, scope, quality, and schedule. For example, it would consider what would happen if the budget were depleted or if a natural disaster occurred.

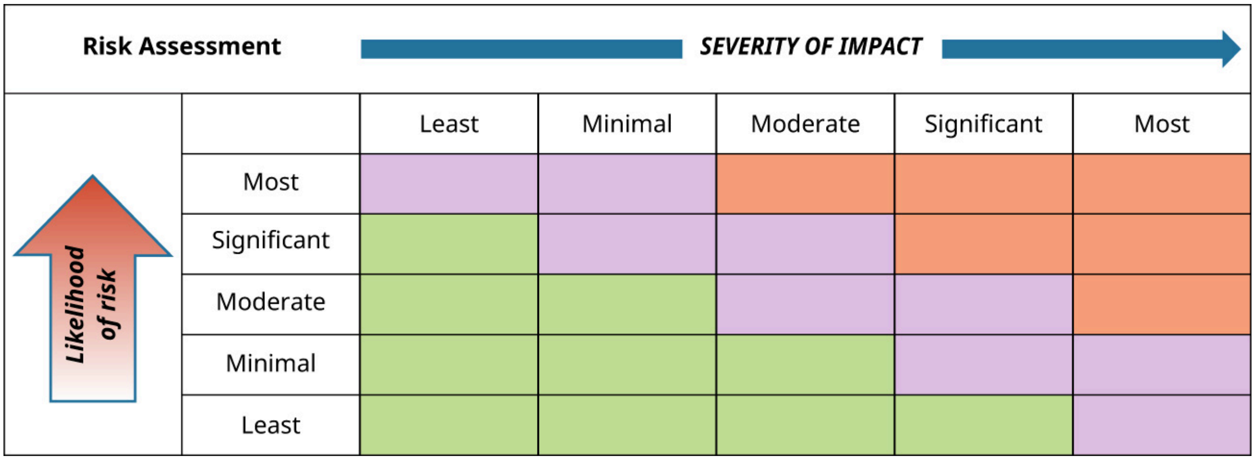


Figure 9.15 A risk assessment matrix can help project managers determine the level of impact of a risk by accounting for its probability and severity. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

For easy evaluation, the impact of a risk can be sorted across categories, such as the range from least to most in Figure 9.15. The likelihood of a risk (for example, an earthquake on the East Coast of the United States) happening is called the probability, which ranges from least to most. An earthquake on the East Coast of the United States has a least probability because history tells us this does not happen very often. The severity of the impact of a risk on a project's cost, schedule, scope, and quality is also measured from least to most. A **risk register** documents the risk to the project being completed within budget, on time, within scope, with good quality, and with minimal risks. Figure 9.16 shows how a risk could be ranked. The project manager would then determine if the risk must be accepted or mitigated—or if it is so great that the project should be canceled.

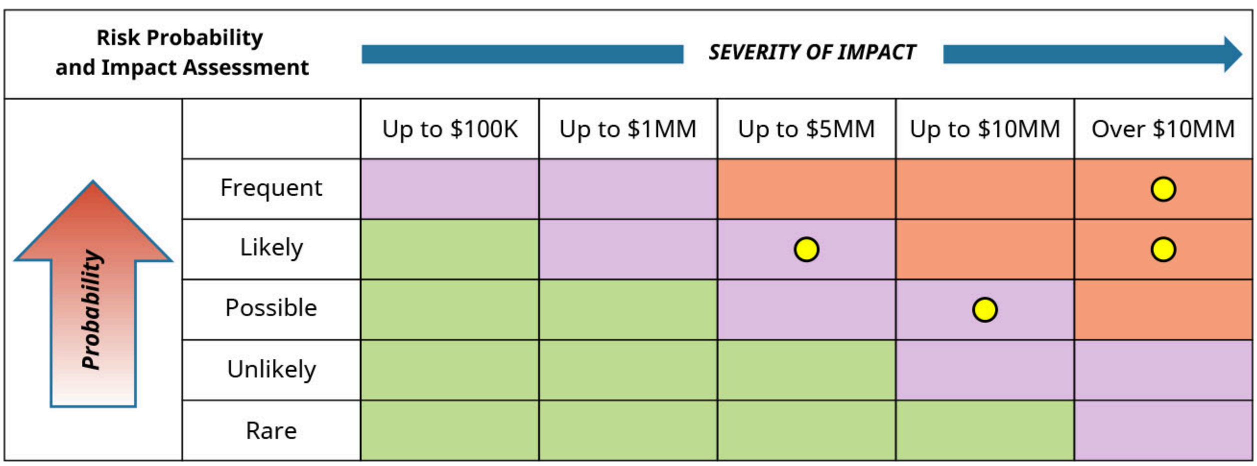


Figure 9.16 As part of a risk assessment, a project manager would use a matrix to determine the risk level of a project and record the risks using a risk register. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

The project manager assesses the probability and impact of risks with respect to the project. This is a hard task, especially for those lacking history or experience in this area or knowledge of disaster events like earthquakes. Here are some tips and a breakdown of the process to use when assessing the probability and impact of risks on your project[3] :

- Probability assessment: Evaluate the likelihood of each identified risk event happening. This can be done qualitatively by assigning probabilities (low, medium, high) or quantitatively by using historical data or statistical analysis to estimate the probability. The probability will be expressed as a percentage.
- Impact assessment: Determine the potential consequences or impact that each risk event can have on the project, such as scope, schedule, budget, quality, and stakeholders. Assess the weight of these impacts

3 Megan Bell, "How to Use a Risk Matrix in Project Management," Project Management Academy, August 24, 2022, https://projectmanagementacademy.net/resources/blog/risk-matrix/#what-is-risk-matrix

based on their severity and significance to the project. For example, if a project that is to be undertaken in a war zone or during the monsoon season, there will likely be some major risks to the project both in completing the project and in protecting the human resources who are performing the tasks on the project.

- Prioritizing risks: Prioritize risks based on their significance to the project. Prioritization will help you allocate resources so you can focus on managing the most critical risks. Known as risk scoring or ranking, the project manager assigns scores or ranks to each risk based on its evaluated probability and impact. For example, consider a project located in the polar ice caps during the winter season. The risk of getting enough goods and materials to this region is high in the coldest part of winter. This might be ranked as a high risk. Various techniques, such as risk matrixes, decision trees, or multicriteria decision analysis, can help evaluate these risks. The higher the score or rank, the greater the priority of the risk.
- Consideration of project objectives: Take into account the project's specific goals, constraints, and priorities when prioritizing risks. Some risks may be more critical to achieving project success, while others may have a lower impact on overall objectives. An example would be a slowdown in the supply of materials to complete a project, such as silicon chips due to a major pandemic, or finding human resources to complete the project. The project would fail without either of these resources, so the project manager must plan for these obstacles and ensure there is time in the schedule to overcome or mitigate these risks.
- Review and refinement: Always regularly review and refine the prioritization of risks as new information becomes available or project circumstances change. This is critical because risks and situations can change frequently. For example, you could be at the end of a project when you realize your team doesn't have a certain kind of tool to finish the highly technical assembly of some part. To help prepare for this, reassess the priority of risks at key project milestones or decision points to ensure that risk management remains aligned with project needs.

Risk evaluation is an ongoing process that requires continuous monitoring and review throughout the PLC. Following are some simple ways to continuously evaluate risks:

- Continuous monitoring: Continuously monitor the status of identified risks and track any changes in their probability or impact. Conduct regular risk assessments, status updates, and progress reports, and obtain stakeholder feedback.
- Periodic reviews: If you have a project that doesn't have very many high-level risks, you might be able to conduct periodic risk assessments to reassess the evaluated risks and their prioritization. Along with this, review the effectiveness of existing risk mitigation measures and identify any new risks that may have emerged.
- Adjustments and updates: If you evaluate and measure each new development as it comes into the project, you likely encounter adjustments and updates. For example, maybe you have a change order. This would be a good time to adjust the risk assessment. You would adjust risk evaluations and priorities based on the current situation and any new project developments, and you would update risk response strategies, mitigation plans, and contingency measures to address any changes in the risk landscape.

Mitigating Risks

Mitigating project risks is a crucial aspect of risk management. It involves taking proactive measures to reduce the probability and impact of the risks that have been identified and evaluated. For example, suppose a project involves doing construction work during the monsoon season in Africa. Since there is very little rain in parts of Africa at most times, the project team might be able to mitigate this risk by scheduling around the monsoon season. Some risks may not be as easy to mitigate. In those cases, the project manager, along with the organization's leadership, will need to determine how much risk the organization is willing to accept on the project. There are several strategies that can help project managers enhance their ability to navigate potential obstacles and improve project outcomes.

Developing Risk Response Strategies

Once a project manager has identified and evaluated the risks associated with a project, the next step is to develop risk response strategies. These strategies define the actions to be taken in response to specific risks:

- Avoidance: Identify risks that can be completely avoided by taking specific actions. You cannot avoid all risks, but if you can, do so. For example, if a project is at risk of exceeding the budget due to scope creep, establishing strict change control processes can help avoid unnecessary scope changes.
- Transfer: If you cannot avoid a risk, then consider risks that can be transferred to external parties. This can be achieved through contractual agreements, insurance policies, or outsourcing certain project activities to specialized vendors or partners.
- Mitigation: If other steps fail, implement measures to reduce the probability or impact of the risks. This may involve implementing additional quality control processes, conducting regular inspections, or enhancing project team skills through training.
- Acceptance: If a risk cannot be avoided, transferred, or mitigated, accept the risk and prepare for any consequences. Acceptance involves acknowledging the risk and its potential impact while developing contingency plans to address any adverse effects.

Implementing Risk Mitigation Measures

Implementing mitigation measures ensures that the identified risks are effectively addressed. The project manager would need to be sure that all stakeholders are aware of the risks and that the individuals responsible for mitigation measures are involved in the risk process. Clearly define roles and responsibilities for implementing risk mitigation measures. Assign specific team members or stakeholders to oversee the execution of mitigation actions. The project manager could do this, but it is most likely that another team member or leadership can resolve the issues. The project manager would still need to follow up and ensure the risk is mitigated to everyone’s satisfaction.

Next, develop a contingency plan. Identify potential fallback options or contingency plans to address risks that cannot be completely mitigated. A **contingency plan** outlines the actions the project manager would take if the risky event occurred, allowing for a quick and efficient response. Some companies may already have responses to these risks in their overall operations plan. Be sure that all stakeholders, including members of the leadership team, clients, and others, are aware of contingency plans. Communication is key in risk management, and when risk occurs, it can play a role in whether the end result is a successful project or one that goes wrong.

Finally, monitor and track the risks to be sure to mitigate them in the future. Continuous monitoring is needed to measure the effectiveness of the mitigation plan. Regularly track the status of risks, assessing whether the planned actions are reducing the probability or impact as intended.

Regularly Reviewing and Reassessing

Risk reviews are an ongoing process. It is important to adapt and refine mitigation strategies as circumstances continuously change. As a project manager, it is your job to ensure that these risks are constantly being reviewed and reassessed. Besides doing periodic reviews, focus on lessons learned from other projects where similar risks may have occurred. If you can capture and document these risks during a lesson learned, it could save you a lot of time and money on newer projects. Review your own projects’ risks from previous projects and see how these risks impacted your project and then determine if there would have been a different solution that you could have applied. Regardless of the process or methodology you choose, you must stay on top of managing risks so your project goes as smoothly as possible.

9.3 Career Focus: Opportunities in Information Systems Project Management

Learning Objectives

By the end of this section, you will be able to:

- Determine career opportunities in the field of project management
- Explain what responsibilities, requirements, and characteristics are needed to be a project manager

Project management in IS can be a rewarding and fulfilling career with a lucrative salary for a college graduate of any age or level of experience. When looking at careers in certain fields like health care or IT, consider combining industry experience with a few courses or training in project/program management to enhance career pathways in these fields and increase potential earnings.

Career Opportunities in Project Management

Project, program, and portfolio managers are all highly skilled individuals with expertise in managing projects, programs, and portfolios. Combining these skills with another expertise allows you to expand your career possibilities and earning potential. Project managers are needed in a variety of fields and industries, including business, manufacturing, engineering, IT, finance, education, health care, and logistics, among others. You will find many of these types of jobs on internet job boards. Explore PMI.org to find many articles, job announcements, and career resources that can help you plan your future and provide valuable project management tips for your life right now. Many roles and positions require project management training but do not hold the title of a project manager. Following are some of the career opportunities in IS project management:

- project manager
- program manager
- portfolio manager
- business analyst
- IT consultant
- technical project manager
- IT operations manager
- risk manager
- Agile coach
- scrum manager

Each of these positions stems from the training or education you receive as a project manager. As an IS professional, you may not want to be an analyst or data manager or a network architect in the IT sector. You might prefer the management side of IS. If so, a strong background in project management will give an entry-level candidate an advantage over many other IS professionals.

Practical experience is crucial for project managers. You can start building experience by looking for internships or co-op programs in project management or related roles. Your college or university institution or a career department can assist you in finding these types of internships. You can also reach out to smaller companies that may need that expertise and are willing to help reimburse tuition if you work with them during the summer and after graduation. These experiential learning opportunities allow you to apply theoretical knowledge in real-world situations, understand project life cycles, work with diverse teams, and gain exposure to project management methodologies and tools. Entry-level positions in project coordination or assistant roles can also provide valuable experience. Consider taking on some projects at your institution or with a current employer. This may be beneficial for both you and the organization you are working with.

Project Management in Health Care

Health care is a growing industry worth billions of dollars. There are hundreds of jobs for individuals who study health care, but there are also many jobs for those who have degrees in other areas like project management (Figure 9.17). Here are a few interesting positions that combine health-care management and project management in the health-care industry:

- Health-care project manager: This is a general project management role focused on overseeing and managing projects within health-care organizations. Health-care project managers may work on initiatives related to process improvement, technology implementation, facility expansion, or quality improvement. These project managers may have some background in health care or health-care systems.
- Information technology project manager: Health-care organizations rely heavily on technology for various purposes, such as electronic medical records, telehealth systems, and data analytics. Information technology project managers in health care are responsible for managing technology-related projects, including system implementations, software upgrades, infrastructure enhancements, and cybersecurity initiatives. Positions in IT project management usually have higher salaries than other project management positions in health care.
- Clinical project manager: Clinical project managers oversee projects related to clinical research, trials, or the development and implementation of new medical procedures or protocols. They work closely with clinical researchers, physicians, and regulatory bodies to ensure compliance, manage timelines, and monitor progress. These positions usually require a health-care background or degree. Many nurses advance to positions like these with the proper project management training.
- Health-care informatics project manager: With the growing importance of health information systems and data analytics in health care, informatics project managers are responsible for projects related to data integration, data warehousing, data analysis, and health information exchange between doctors, hospitals, and other providers. They collaborate with many teams throughout the organization to ensure efficient and secure management of health-care data. Any position in informatics usually requires a background in informatics or health care.
- Quality improvement project manager: Quality improvement is a critical aspect of health care, and project managers in this role focus on projects aimed at enhancing patient care, safety, and overall quality. Individuals in these positions are usually highly trained in health-care operations. They work on initiatives such as implementing evidence-based practices, developing quality metrics, and leading process improvement efforts. A lot of nurse leaders find themselves in positions like this after obtaining their master's degree in leadership.
- Compliance project manager: Compliance with regulations and standards is essential in health care. Compliance project managers ensure that health-care organizations meet regulatory requirements, such as HIPAA, GDPR, and industry-specific requirements. Because compliance project managers develop compliance programs, conduct audits, and implement measures to mitigate issues, these positions usually require experience in compliance.

Figure 9.17 The health-care industry supports a wide range of project management positions. (credit: modification of work "NMCP Holds Nursing Skill Fair 211021-N-MY642-1009" by Navy Medicine/Flickr, Public Domain)

These are just a few of the positions you can hold in the health-care industry as a project manager with a medical or health-care background. It's important to read the job responsibilities for positions like these to determine the specific requirements and expectations.

Project Management in Finance

The financial industry also employs many different graduates from all types of background and degree programs. The financial industry is vast and ranges from small-town banks to large global investment firms. Depending on your expertise, experience, and the specific needs of the organization, you will find that project managers are paid very well in this industry. Following are some of the project manager positions in the financial industry:

- Banking project manager: Like a health-care project manager in health care, this is a general project management position responsible for overseeing and managing projects across different areas of the bank. This may include projects related to process improvement, system implementations, regulatory compliance, customer experience enhancements, or product/service launches. Any project that requires scheduling, budgeting, quality, and risk oversight would be a job for a project manager.
- Information technology project manager: Just as in health care, banks heavily rely on technology to provide secure services. Security and privacy are the most important responsibilities when dealing with people's money. Information technology project managers in the financial industry manage many high-tech projects, such as banking system upgrades, software development, cybersecurity initiatives, digital transformation projects, AI, data analytics, and infrastructure enhancements.
- Risk management project manager: Risk management is an important aspect of banking operations. Project managers are well equipped to handle risks and evaluate probability and impacts. In general, risk management project managers focus on projects related to identifying, assessing, and mitigating risks. They work on projects such as implementing risk management frameworks, regulatory compliance projects, operational risk mitigation initiatives, disaster management, or business continuity planning. Individuals in this position usually have a strong background in IT or security.
- Digital banking project manager: With the rise of digital banking services, project managers in this role focus on projects related to digital transformation, online banking platforms, mobile banking applications, and digital payment solutions. They oversee projects that aim to enhance customer experience, increase self-service capabilities, and drive digital innovation within the bank. Digital project managers are becoming more popular in all industries but especially in banking.
- Regulatory compliance project manager: Banks operate within a highly regulated environment. Regulatory compliance project managers ensure that the bank adheres to applicable laws, regulations, and industry

standards. They manage projects related to compliance with financial regulations, anti–money laundering initiatives, and data privacy regulations. In these positions, a project manager would need to have a background in regulatory matters and compliance in the financial industry.
- Product development project manager: Banks continuously develop and launch new products and services to meet customer demands. Product development project managers lead development initiatives of new products and could oversee a portfolio of projects in the development area. Usually these project managers collaborate with cross-functional teams to ensure successful product delivery. This is a great position for a project manager who is very creative and likes to be on the cutting edge of product development.
- Merger and acquisition project manager: In the financial industry, mergers, acquisitions, and integrations are common. Usually there is a separate merger and acquisition department that handles the merger and acquisition of companies interested in buying or investing in other companies. Usually, these positions are found in large investment brokerage companies that solely manage mergers and acquisitions. Project managers specializing in this area perform due diligence, integration planning, systems consolidation, and cultural alignment tasks. This is a very interesting career for someone who likes to work across various industries.

The financial industry can be a very exciting and lucrative career for anyone who studies business and project management. Even if you don't enjoy math or accounting, a project manager can still be successfully employed in the financial industry.

Project Management in Manufacturing

You may find yourself in a manufacturing industry where administrative and technical jobs are the focus, but where project managers play a significant role (Figure 9.18). Just as in other industries, project managers can hold various positions depending on the specific needs and projects within the organization. Having an engineering or technical degree or background can support a smooth transition to a project manager position in manufacturing.

Figure 9.18 Many engineers study project management as part of their degree program. (credit: "Tesla Autobots" by Steve Jurvetson/ Flickr, CC BY 2.0)

These positions are common for engineers in manufacturing:

- Manufacturing project manager: A general project management role within the manufacturing sector, these project managers oversee and coordinate projects related to process improvement, product development, facility expansion, equipment installation, and production optimization. They ensure projects are executed efficiently, are within budget, and meet quality standards.
- Lean Six Sigma project manager: Lean Six Sigma is a methodology widely used in manufacturing to streamline processes, reduce waste, and improve efficiency. Lean Six Sigma certified project managers lead projects focused on process improvement, waste reduction, and quality enhancement. They can

make a comfortable living by having a project manager certification and a Lean Six Sigma certification. They work closely with cross-functional teams to implement Lean Six Sigma methodologies and achieve operational excellence.
- New product development project manager: Manufacturing companies often engage in developing and launching new products. New product development project managers oversee projects related to introducing new products to the market. They manage the entire product development life cycle, from concept design to prototyping, testing, and final production. With the manufacturing of any new product, systems are needed to develop the product that takes a long time to produce. This may be a good fit for those who like to be creative and have an engineering or manufacturing background.
- Supply chain project manager: Supply chain project managers focus on optimizing the supply chain processes within manufacturing organizations. Many business majors with a specialization in supply chain work make great project managers in this industry. They work on projects related to supply chain network design, supplier management, logistics optimization, demand planning, and inventory management. They collaborate with various stakeholders to ensure smooth operations and cost-effective supply chain management. As the world becomes more integrated, supply chain management is expected to be a growing area. Supply chain management can be a very exciting and lucrative career that can take you all over the world. Project managers in this field can experience the same global career potential. Individuals in supply chain management come from many backgrounds and degree programs, like business, engineering, management, IT, and IS.
- Quality assurance/quality control project manager: Companies can't manufacture or supply products without quality control. Quality project managers oversee projects related to quality assurance and quality control. They establish and implement quality standards, develop quality management systems, conduct audits, and drive continuous improvement initiatives to enhance product quality and customer satisfaction. This role is a good match for those who want to be leaders and have good attention to detail.

Project Management in Engineering

Engineers can be employed in many different types of industries, so it may not be surprising that project managers with an engineering background are highly sought after (Figure 9.19). If you decide to study engineering, you may also want to have project management experience to boost your position and value to the organization. Having the expertise to manage scope, schedule, costs, risks, and quality are skills that every engineer must learn.

Figure 9.19 Project management and engineering usually go together as engineers will be asked to lead projects as part of the job. (credit: "Flickr - Official U.S. Navy Imagery - A Navy engineering technician and the project manager for Pearl Harbor Naval Shipyard review installation plans for a 20,000-square-foot rooftop photovoltaic system" by Marshall Fukuki, U.S. Navy/Wikimedia Commons,

Public Domain)

Here are some positions that project managers can have in the engineering industry:

- Engineering project manager: This is a general project management role within the engineering industry. Engineering project managers oversee and manage projects related to infrastructure development, construction, product design and development, research and development, and engineering consulting. They are responsible for project planning, coordination, resource allocation, risk management, and ensuring successful project delivery.
- Construction project manager: Construction project managers specialize in managing projects within the construction industry. They oversee the planning, execution, and completion of construction projects, including building construction, infrastructure development, and renovation projects. Construction project managers coordinate with architects, engineers, contractors, and other stakeholders to ensure projects are completed on time, are within budget, and meet quality standards.
- Product development project manager: Product development project managers focus on projects involving the design, development, and launch of new products. They work closely with engineering teams, product designers, and marketing teams to define project scope, develop project plans, allocate resources, and manage the product development life cycle from concept to market launch.
- Research and development (R&D) project manager: R&D project managers lead projects focused on research, innovation, and development of new technologies, products, or processes. They collaborate with engineers, scientists, and researchers to define project goals, allocate resources, manage timelines, and ensure the successful execution of R&D initiatives.
- Systems engineering project manager: Systems engineering project managers oversee projects that involve complex systems integration, such as developing and implementing large-scale engineering systems or infrastructure. They coordinate activities across multiple engineering disciplines, manage project scope, ensure effective communication among stakeholders, and drive the integration and successful delivery of complex engineering systems.

Project Management in Business

Business majors are always in high demand to lead and manage some of the most influential companies in the world. Before you become a leader in business, you first must demonstrate your ability to manage and lead projects. A solid foundation in project management enhances any career choice, but in business, this is even more important (Figure 9.20).

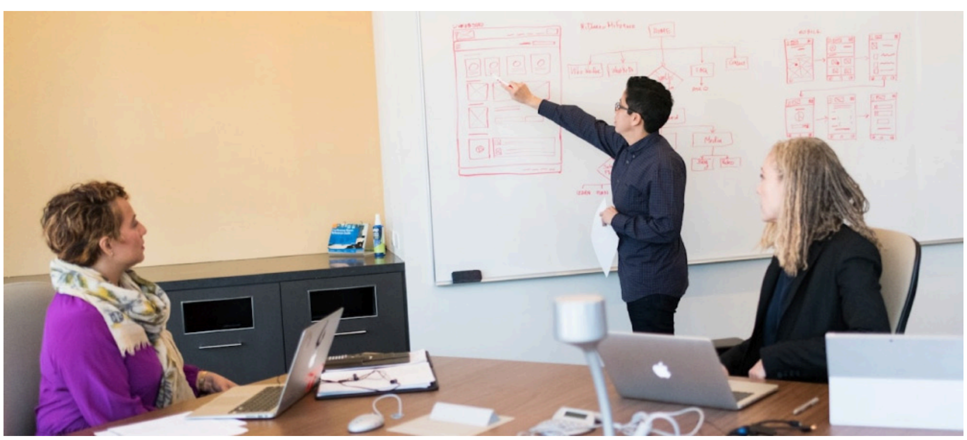


Figure 9.20 Business employs a vast number of individuals with various jobs, skills, and experience. Project management is just another skill set that can easily be part of any job or career for any business in the world. (credit: modification of work “wocintech-microsoft” by WOCInTech/nappy, Public Domain)

Here are some common positions that project managers may have in the business sector:

- Business project manager: This is a general project management role within the business field. Business project managers oversee and manage projects across various business functions, including marketing, operations, finance, human resources, and strategic planning. They ensure project goals are achieved, coordinate resources, manage project schedules, and monitor project budgets.

- Information technology project manager: Information technology project managers specialize in managing projects related to IT or IS technology infrastructure upgrades, integrations, network installations, cybersecurity initiatives, and other IT-related projects. They collaborate with cross-functional and matrixed teams, stakeholders, and external vendors to ensure successful project delivery.
- Marketing project manager: Marketing project managers focus on projects related to marketing campaigns, product launches, brand development, and market research. They coordinate the planning, execution, and monitoring of marketing initiatives, including advertising campaigns, digital marketing projects, social media campaigns, and market research studies. They often are knowledgeable in topics like search optimization and website analytics.
- Operations project manager: Operations project managers are responsible for managing projects that improve operational efficiency, streamline processes, and optimize supply chain management operations within a company. They oversee projects related to process improvement, inventory management, logistics optimization, and operational cost reduction.
- Strategy project manager: Strategy project managers are involved in projects related to strategic planning, business development, and organizational growth. They work on initiatives such as market analysis, competitive research, mergers and acquisitions, and strategic partnerships. Strategy project managers facilitate the development and execution of strategic initiatives to drive business success.

What It Takes to Be a Project Manager

Now that you've learned about the processes, theories, and skills involved in project management, and which industries employ project managers, let's explore what it takes to get a job as a project manager. The main responsibilities of a project manager are to:

- Plan, execute, and monitor projects from initiation to completion, ensuring adherence to project scope, timeline, and budget.
- Develop and maintain project plans, including resource allocation, task assignments, and milestone tracking.
- Coordinate and communicate with cross-functional teams, stakeholders, and clients to gather project requirements and ensure project goals are achieved.
- Identify and manage project risks, issues, and changes, implementing appropriate mitigation strategies.
- Track project progress, prepare status reports, and conduct regular project meetings to provide updates and address concerns.
- Manage project budgets, including cost estimation, expenditure tracking, and financial reporting.
- Ensure that project deliverables meet quality standards and stakeholder expectations.
- Foster a collaborative and positive project culture, motivating team members and promoting effective teamwork.
- Maintain documentation, project files, and lessons learned for future reference.

Project management training or degree programs focus on developing skills for the responsibilities required and teaching students how to perform these tasks. The responsibilities are fundamental skills that project managers must perform and perform well to be within budget, scope, and costs while maintaining quality and accounting for risks.

Following are some requirements of a project manager position[4]:

- bachelor's degree in a relevant field (such as business, engineering, or computer science) or equivalent work experience

4 "Project Manager Job Description: Top Duties and Qualifications," Indeed For Employers, updated January 13, 2025, https://www.indeed.com/hire/job-description/project-manager

- proven experience in project management, including planning, executing, and delivering projects on time and within budget
- strong leadership and communication skills, with the ability to effectively manage teams and stakeholders
- excellent organizational and time management skills to prioritize tasks and meet deadlines
- analytical and problem-solving abilities to identify and resolve project challenges
- proficiency in project management software and tools
- project management certifications such as Project Management Professional (PMP) or Certified Associate in Project Management (CAPM)

A wide range of bachelor’s degrees can qualify for this position. They include business, engineering, or computer science, along with a PMP or CAPM certification. No matter what you may study in college or through training, you can always add more training or skills in project management to increase your value in the market.

Characteristics of Project Managers

Project managers possess a range of characteristics that contribute to their success in leading projects. Here are some characteristics typical of successful project managers:[5]

- Leadership: As a project manager, you need strong leadership skills to guide teams, to inspire, collaborate, and motivate individuals to achieve project goals. You must also be able to provide clear direction, delegate tasks, and foster a positive and productive work environment.
- Communication: Effective communication is necessary for project managers to convey information, set expectations, and facilitate effective collaboration among team members, stakeholders, and clients. Project managers are skilled in active listening and clear verbal and written communication and are able to adapt their communication style to different audiences.
- Organizational skills: Project managers must be highly organized to handle multiple tasks, deadlines, and resources effectively. Project managers develop detailed project plans, establish timelines, allocate resources, and track progress to ensure projects stay on track and within budget.
- Problem-solving skills: Project managers encounter various challenges throughout projects. You should possess strong problem-solving skills to identify issues, analyze root causes, and develop effective solutions. You should be proactive in mitigating risks, handling conflicts, and making timely decisions to keep projects on course.
- Adaptability: Projects often require flexibility and adaptability as circumstances change. You can expect that all projects have their challenges, and you need to think fast and adapt to those changes. Project managers can adjust their plans, resources, and strategies to accommodate unforeseen challenges or shifting priorities.
- Collaboration: Even though the project manager has a lot of control and authority, a project manager is part of a team aiming to get projects completed through collaboration. Project managers work with cross-functional teams, stakeholders, and external partners. A project manager needs to excel in building relationships, fostering collaboration, and promoting teamwork.
- Time management: Managing your time and your team’s time is a priority for project managers. Project managers are adept at managing time efficiently. They prioritize tasks, set realistic deadlines, and ensure project milestones are achieved on time.

Many of these characteristics are soft skills required of any career. Colleges and universities pay close attention to developing these skills in their students. Characteristics like leadership, collaboration, and time management are all key skills for project managers and are taught in any project manager program.

Developing foundational skills is a good way to achieve success as a project manager. You may discover you are very good at these skills already, and you don’t have to wait to practice them. Try applying budgeting,

5 Thanos Markousis, “Project Manager Job Description,” Resources for Employers, updated February 1, 2022, https://resources.workable.com/project-manager-job-description

scheduling, and time management skills into your daily life. Seek out internships to get experience. Sign up to run a project for a student organization or take on a leadership role and focus on managing the organization and projects using best practices and skills you learned in your studies. Always seek out opportunities for teamwork and collaboration no matter where you are in life or where you may find the opportunities.

Education and Certifications to Become a Project Manager

A specific degree is not required but having some courses or training in project management or a related field can be advantageous. Pursuing a bachelor’s or master’s degree in fields such as business administration, engineering, computer science, or project management can provide an understanding of the principles and fundamentals of project management. Courses in specialty areas like IS offer opportunities to learn about project management methodologies, tools, and best practices through case studies and group projects.

Project management certifications can enhance your credentials and earning power, as well as demonstrate your commitment to the field. The PMP certification, offered by the PMI, is one of the most recognized and respected certifications in the industry. To earn the PMP certification, you need a combination of education and project management experience, along with passing the PMP certification exam. If you don’t have enough experience to get the PMP certification, which requires three to five years of demonstrated project management work, you may want to consider a CAPM certification, which only requires two years of demonstrated experience in project management. Having demonstrated experience in project management doesn’t mean you have to have held the title of a project manager, only that you have performed various tasks in project manager task areas like initiating, managing, and closing projects. Both PMP and CAPM certifications require an individual to have a fixed number of hours of training before taking the exam, and they also require continuous professional development and ongoing training to maintain both certifications. PRINCE2 certification can also be pursued to showcase your knowledge and skills in project management. It also requires demonstrated experience in project management, an exam, and continuous professional development.

Many project management positions will require some sort of certification. To obtain the best credentials in project management and earn the most in salary for the job, you will likely need a PMP certification or a certification in a specific Agile project management area like Scrum Master or PRINCE2.

Project management is forever evolving, and staying updated with the latest trends, methodologies, and tools is important to maintain your certification and your expertise. As you complete college or training, you should think of learning as a lifelong endeavor. New technologies, new tools, and new best practices are progressing at a faster rate than ever before. Adopting a mindset of continuous learning and professional development is a must for long-term growth and sustainability. Attending industry conferences, workshops, and seminars, as well as engaging in online resources, webinars, and reading project management publications are all methods of continuous learning. Joining professional organizations and networking groups is a great way to connect with experienced project managers and learn from their experiences.

GLOBAL CONNECTIONS

Global Outlook on Project Management

According to PMI.org, demand for project managers through 2027 will grow faster than demand for other occupations. Through Anderson Economic Group (AEG), PMI conducted a study of job opportunities and growth associated with project management that covered eleven countries including the United States. The study revealed that through 2027, project management positions in the top seven industries will grow by 33 percent, producing twenty-two million new jobs around the world. By 2027, employers will need around eighty-eight million individuals in project management. For example, in the United States, the Bureau of Labor Statistics projects the employment of project management specialists to grow by 7 percent between 2023 and 2033.[6] The countries with the most need for project managers will be China and India, together representing more than 75 percent of the total project management positions. Organizations are seeing the need for more project managers as productivity continues to grow.[7]

6 Bureau of Labor Statistics, "Project Management Specialists," *Occupational Outlook Handbook*, U.S. Department of Labor, last modified August 29, 2024, https://www.bls.gov/ooh/business-and-financial/project-management-specialists.htm

7 Project Management Institute, *Project Management Job Growth and Talent Gap 2017–2027* (Project Management Institute, 2017), https://www.pmi.org/learning/careers/job-growth

Key Terms

adaptive development approach development approach that provides a framework that enables project team members to repeat the processes of cycle planning and task initiation as needed

Agile project management type of project management that involves taking an iterative and incremental approach to delivering projects

change management process proper procedure for stakeholders to change or modify the scope of the project

contingency plan outlines the actions you would take if a risky event occurred

escalation policy determines when the project manager should report budget issues, such as being under or over budget

extreme programming (XP) Agile methodology that emphasizes the use of software engineering practices to improve quality and responsiveness

incremental development approach development approach that enables a project to be divided into parts, or increments, that work together and build on each other

Kanban Agile framework that helps managers visualize and optimize the flow of work through a visual representation of the tasks and how they flow through the project

portfolio management centralized management of a set of projects grouped together to identify, prioritize, authorize, and control the related work

predictive development approach development approach useful for projects that have specific requirements with well-defined goals and objectives

PRINCE2 (Projects in Controlled Environments) project management methodology and certification process that is widely recognized around the world

program management coordinated organization, direction, and implementation of a group of related projects to achieve outcomes and realize benefits that are strategically important to the business

project temporary initiative or endeavor to create a product, service, or result that has a beginning and end date

project charter formal document that authorizes project initiation

project closure stage at which the project comes to a formal conclusion, ensuring that all project objectives are met and deliverables are handed over

project development process of planning a project and ensuring that it has the resources necessary to successfully achieve its goals and objectives

project execution stage that involves implementing the project plan, managing resources, and monitoring progress

project initiation stage at which a project is created and involves defining its purpose, objectives, and stakeholders

project life cycle (PLC) development, monitoring, and control of a project

project management use of specific knowledge, skills, tools, and techniques to provide guidance through each stage of a project

Project Management Body of Knowledge (PMBOK) guide for handling projects using a systematic methodology and proven processes for initiating, planning, executing, managing, monitoring, and closing a project

Project Management Institute (PMI) accrediting body for the project management process that certifies project managers, program managers, and portfolio managers

project management office (PMO) department within an organization that provides the standards and guidelines to project managers for projects and governs how projects are initiated, planned, organized, implemented, managed, and closed

project manager (PM) person who applies knowledge of project management and uses various tools and techniques to initiate, plan, execute, monitor, control, and close projects

resource planning task of determining what resources are needed and when they will be needed for the project

risk event or condition that has a negative effect should it occur during a project

risk management process that encompasses risk identification, qualitative and quantitative analysis, risk response planning, and risk monitoring and control

risk register document in which the results of risk analysis and risk response planning are recorded

scope deliverables, objectives, and requirements of the project

scope creep scope of the project grows beyond what was agreed to in the planning stage of the project as requirements are changed or modified

scrum Agile framework that focuses on delivering value through small, cross-functional teams working in sprints, and the product backlog contains a prioritized list of user stories or features

scrum master leader of the scrum meeting

stakeholder analysis review and evaluation of each stakeholder, their background, expertise, and impact on the project

statement of work document detailing the requirements, deliverables, schedule, and responsibilities of the stakeholders of a project to establish a clear understanding of what the project entails

work breakdown structure (WBS) process that helps the project manager understand how the deliverables will be scheduled and any dependencies there might be in completing other deliverables, essentially breaking down a project into smaller, more manageable work packages and tasks

Summary

9.1 Foundations of Information Systems Project Management

- Project management is a multidisciplinary way of ensuring that projects are on time, within budget, and in scope, and that deliverables are of good quality and risks are minimal.
- There are many different project management methodologies, but three of the most well documented are PMBOK (waterfall), Agile, and PRINCE2.
- The three most commonly used approaches for project development include predictive, adaptive, and incremental.
- There are many tools and processes within project management including how to handle stakeholders, review of deliverables, assignment of resources and assets, planning and budgeting for projects, execution strategies, and lessons learned.

9.2 Setting Up and Managing Projects for Success

- There are five stages of a project, and various tasks within each stage make up the project management framework. They are (1) project initiation, (2) project planning, (3) project execution, (4) monitoring and control, and (5) project closure.
- It is important to develop a comprehensive project plan and schedule. This phase of the project involves several key steps, each of which plays a significant role in shaping the project's direction and facilitating efficient execution.
- A WBS helps identify project tasks, dependencies, timelines, and resources needed.
- Effective risk assessment is crucial for managing successful project outcomes.
- A risk assessment is based on defining the risks to a project, evaluating the risks, assigning risk responsibility, and determining the risk mitigation strategy.

9.3 Career Focus: Opportunities in Information Systems Project Management

- There are project managers in many different career paths like business, health care, IT, education, manufacturing, logistics, and more.
- Project management is a field or career where having a specialty area like health care or manufacturing can be an advantage.

- Most positions require a bachelor's degree with experience or knowledge of project management.
- Obtaining a certification in project management will help increase your salary as a project manager and further your career path.

Review Questions

1. What constitutes a project?
   a. an endeavor that is undertaken to create a product or service and has definite beginning and ending dates
   b. the application of knowledge, skills, tools, and technologies to project activities
   c. a portfolio of endeavors managed as a group to achieve strategic objectives
   d. an endeavor of activities that are used to drive value in delivery of products and services

2. What performance domain is best used to help determine the approach to a project?
   a. planning performance domain
   b. team domain
   c. stakeholder domain
   d. development approach domain

3. Which statement best distinguishes between stakeholders and teams in the project management domains?
   a. Stakeholders are part of the team.
   b. The team is part of the stakeholder's domain.
   c. The team is invested in project deliverables.
   d. Stakeholders measure the quality level of a project.

4. Which modifiers best describe the similarities between Agile, PRINCE2, and PMBOK?
   a. iterative and structured
   b. iterative and somewhat structured
   c. somewhat iterative and unstructured
   d. somewhat iterative and mostly structured

5. What are the first three steps in developing a project plan?
   a. Define the scope, determine the budget, and determine the resources.
   b. Define the scope, determine the budget, and assess the risks.
   c. Assess the risks, define the scope, and determine the resources.
   d. Determine the budget, determine the resources, and assess the risks.

6. Identify the five main stages in developing and managing a project.
   a. project initiation, project schedule, project execution and monitoring risks, and project closure
   b. project charter, project planning, project implementation and monitoring, and project closure
   c. project initiation, project planning, project development and monitoring risks, and project closure
   d. project initiation, project planning, project execution, monitoring and control, and project closure

7. What steps are included in the execution portion of a project?
   a. coordinating resources, managing risks, resolving issues, and ensuring quality control
   b. assigning all resources, monitoring risks, maintaining the schedule, and setting up quality control measures
   c. managing resources, monitoring risks, resolving the schedule, and measuring quality control
   d. monitoring resources, managing risks, fixing issues, and guaranteeing quality control

8. How do career opportunities in project management change depending on the field you go into?
   a. Some positions require a degree in project management.
   b. Some positions only require a certification or training in project management.

c. Some positions require a background in the specific industry or field of study (such as health care).
d. Some positions remain the same regardless of the industry in which you have experience or background.

9. Which certification is the most widely recognized and required for many project management jobs?
   a. Project Management Professional from Project Management Institute
   b. Certified Scrum Master from Axelos
   c. Certified Associate in Project Management from Project Management Institute
   d. PRINCE2 certification

Check Your Understanding Questions

1. Explain the project management approaches in the PMBOK (waterfall) methodology and why an organization would choose to use this methodology.
2. Explain the aspects of the planning performance domain and how it impacts the success of the project.
3. Briefly explain each of the project management methodologies: PMBOK, Agile, and PRINCE2.
4. Which stage of a project uses a statement of work? Define the statement of work and explain how it is used during this stage.
5. What is a work breakdown structure and how does it help a project manager?
6. Why is it important to include stakeholders in risk assessment and management? How can stakeholders be engaged?
7. Consider a recent college graduate in business with a minor in finance. They have some project management training but do not have a certification. They really like to get into the details surrounding regulations and laws and find research to be enjoyable. Which career(s) in business should they pursue that include project management, and why?
8. Explain how a career as a project manager in manufacturing and a career as a project manager in engineering are similar.
9. Read this summary of a project manager position in health care. Explain which characteristics of a project manager would be most beneficial in a role like this and why.

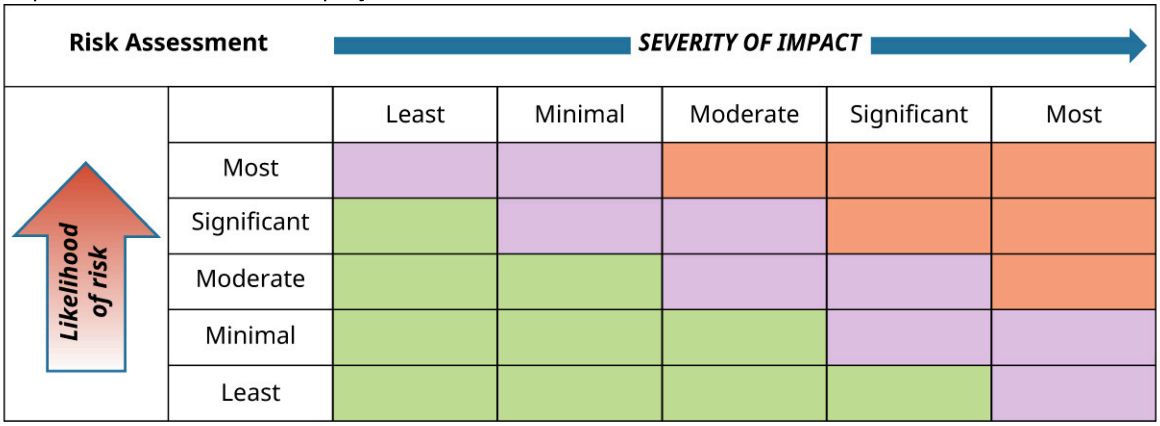
   Quality Improvement Project Manager: Quality improvement is a critical aspect of health care, and project managers in this role focus on projects aimed at enhancing patient care, safety, and overall quality. Individuals in these positions are usually highly trained in health-care operations. They work on initiatives such as implementing evidence-based practices, developing quality metrics, and leading process improvement efforts.

Application Questions

1. If you were a project manager, which of the eight performance domains of project management do you think you would excel at and why? Also, which of the eight domains would you need to work at and why?
2. Develop a short project management scenario like the case study featured in this chapter where the best development approach would be the incremental approach.
3. Develop a short video or slide presentation that explains the concept and structure of a project management office and provide examples that illustrate the differences between project, program, and portfolio management.
4. You are a project manager for a hospital in the human resources department. The human resources team

is having trouble staffing radiology technicians. The vice president of human resources has called a team together to discuss the initiation of a project to hire or outsource more radiology technicians. The vice president asks you to lead the project. You meet with the team to begin planning for the project. One team member speaks up to ask: “How are we going to hire or outsource technicians when there is a shortage across the country of these individuals?” This brings up a discussion about the risks of the project.

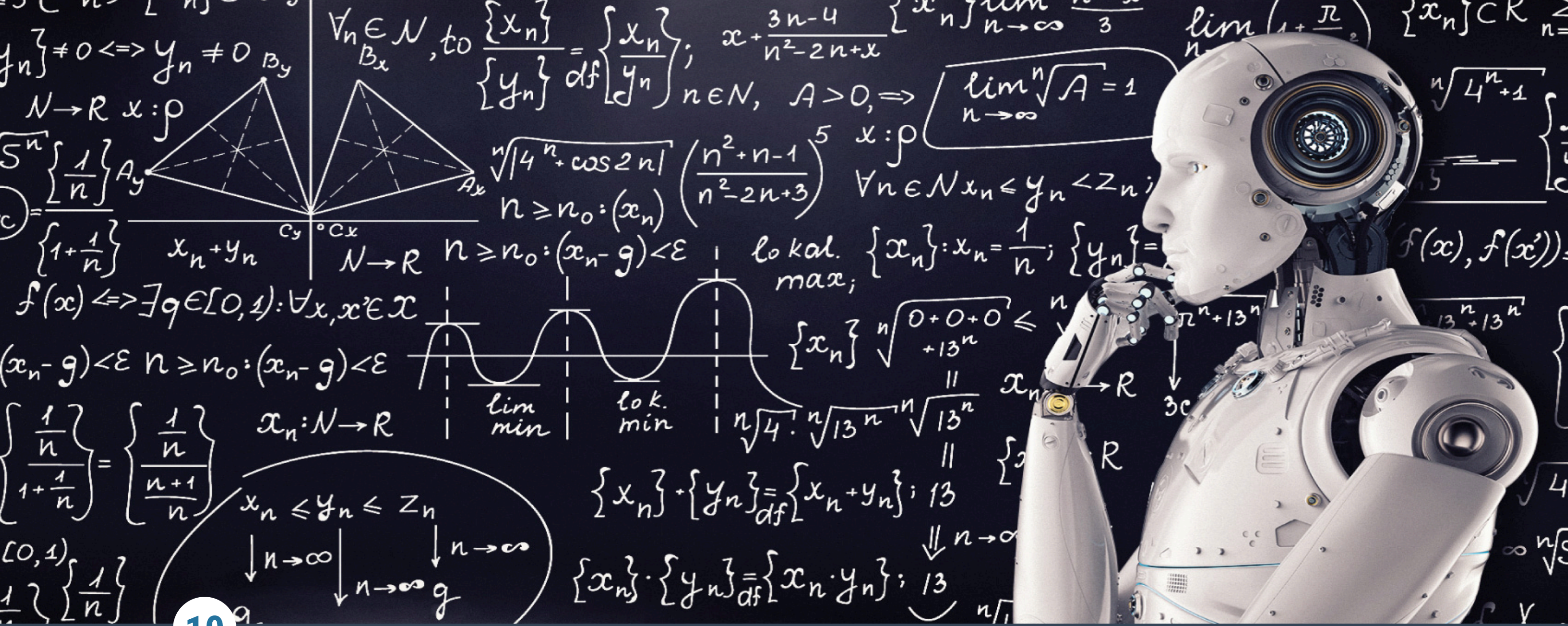
a. Come up with the top two risks associated with this project to deliver radiology technicians to fill the open positions and explain your reasoning for why this is a risk.
b. Evaluate the risks you determined in the previous exercise. Fill in the risk register to determine the impact of those risks on the project.



c. Prepare a brief recommendation on how to mitigate the risks you discovered and evaluated. If all the risks cannot be mitigated, provide a brief explanation as to why they cannot be mitigated and offer alternatives.
d. Explain how these risks will impact the project’s costs, schedule, scope, quality and risk of the project.

5. Considering your background, education, and experience, explain which industry you would be better suited to have a position as a project manager, and explain which type of project manager you would like to be.

6. Go to a job search board like Indeed.com or CareerBuilder.com. Search for a project management position in business, health care, engineering, manufacturing, or finance. Read the job description and qualifications. Do an analysis of your resume and the qualifications for the job. Determine the gaps in your education, background, and learning in project management and describe how and where you can obtain the skills you still lack.



10 Emerging Technologies and Frontiers of Information Systems

Figure 10.1 Robotics and their growing ability to process large volumes of data remain central to discussions on emerging technologies. (credit: modification of work "Artificial Intelligence & AI & Machine Learning – 30212411048" by https://www.vpnsrus.com/Wikimedia Commons, CC BY 2.0)

Chapter Outline

Introduction

Innovation can be defined as applying a new process or concept to an existing technology to add value, enhance its capabilities, improve efficiency, or address unmet needs. Innovation is continually applied to technology, resulting in emerging technologies that create opportunities, challenges, and risks. Ultimately, these technologies can significantly impact individuals and organizations.

10.1 Defining Emerging Technologies

Learning Objectives

By the end of this section, you will be able to:

- Define emerging technology and provide examples
- Identify real-world applications of emerging technologies
- Identify the opportunities, challenges, and risks of emerging technologies

When you hear the phrase "emerging technology," what comes to mind? Have you ever driven an electric car or ridden in a self-driving car? What do you think are the factors that determine if a technology is emerging? Would you consider the latest smartphone an emerging technology? Technically, the first commercial smartphone was released three decades ago. If technology created over thirty years ago was emerging then, is it still emerging technology today? What about Henry Ford's historical introduction of the moving assembly line? Both of these technologies were built on existing technologies, and both have been revised and advanced over the years to their current forms—both are examples of the important influences of emerging technologies.

What Makes an Emerging Technology

Any software or hardware that enhances the user experience by obtaining or using information and data in new and compelling ways can be considered an **emerging technology**. The term can be used to describe new technologies or the continuing development of existing technologies. Emerging technology can be found in all areas of our society, including education, information technology, nanotechnology, biotechnology, robotics, and artificial intelligence. If we look back over the last century, there have been many technological advancements: the automated teller machine, the hard disk drive, the magnetic stripe card, mobile telephony, desktop computers, the computer mouse, and more. Each of these was considered an emerging technology at the time and is now a familiar part of our lives.

The progressive nature of emerging technologies allows for companies that embrace them to gain a competitive advantage and the potential for synergies with other technologies that have the same or similar goals. The convergence of technologies has the potential to create efficiencies that may not have previously existed. Consider the convergence of video, voice, and data, for example. All these technologies were new at one time, and as their capabilities became apparent, opportunities became available to combine the technologies for use in one product. Having video, voice, and data on the same network allows multiple forms of communication that are not possible with separate infrastructures. Sending email or text messages to others while having a video chat conversation on the same device used to be hard to imagine, but they are now widely used together.

There are many other forms of technology that are considered to be emerging because of their rapid rate of change. The branch of engineering and computer science called **robotics** involves the conception, design, building, and operation of robots, creating intelligent machines that can assist humans with a variety of tasks. Robotics is considered emerging because it is being used in new and exciting ways every day. For example, many surgeries today are being performed laparoscopically with the assistance of robotic technology. Self-driving and electric vehicles are increasing their presence on roads, making waves in the automotive industry. The Internet of Things (IoT) has introduced biometric scanners and wearable devices that are changing the way we communicate and interact with each other.

Blockchain is considered an emerging technology due to its ability to improve efficiencies and streamline processes across many different industries. A **blockchain** is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets. Blockchains are used for secured, transaction-based actions and information sharing within business networks. Blockchain uses **cryptography**, the process of hiding or coding information so that only the intended recipient can read it. Cryptographic protocols provide secure connections, enabling two parties to communicate with privacy and data integrity and provide additional layers of security. We see examples of blockchain use through the emergence of digital currency, such as cryptocurrency or bitcoin, one type of cryptocurrency. Cryptocurrency uses blockchain technology and allows transactions over the internet with no Federal Reserve System or monetary backing. Blockchain ensures that the cryptocurrency is successfully transferred from the sender to the recipient and arrives at its intended location and that financial transactions occur properly.

In 1977, the U.S. Department of Energy (DOE) was created and charged with promoting broader energy policy, promoting energy conservation, and finding alternative sources of energy. With these goals in mind, the DOE has become one of the largest federal organizations to drive innovation in the areas of power plants, solar panels, and renewable energies, all considered emerging technologies because they influence the way we interact with sustainable resources.

Educational institutions have also provided the means for researchers to foster innovation and develop technology by providing research labs and direct and indirect support, such as funding, research assistants, and faculty with subject matter expertise in research area and statistics. Ivan Sutherland, a professor at

Harvard University, along with his student Bob Sproull, created the first virtual reality (VR) device in 1968 (Figure 10.2). Sutherland is also credited with the development of augmented reality (AR) that same year.

Figure 10.2 Known as the "Sword of Damocles," Ivan Sutherland and his research team created this first head-mounted virtual reality device in 1968. (credit: modification of work "Virtual Reality Headset Prototype" by "Pargon"/Flickr, CC BY 2.0)

Emerging technologies usually introduce novel approaches, concepts, or applications that may not have been previously considered. They also show rapid advancement, developing and changing quickly, often due to an organization's financial investments and research efforts. Other characteristics of emerging technologies include their prominent impact, volatility, complexity, and uncertainty. Additionally, emerging technologies may be characterized by the type of technology used, the industry in which they are used, or the uniqueness of their attributes.

Emerging technologies are also known for their disruptive or transformative potential. They can introduce significant change and challenge traditional norms. For example, the introduction of self-checkout kiosks in grocery stores has reduced the number of cashiers needed to assist customers with their purchases. Following are some other cutting-edge emerging technologies that merit special attention for their transformative potential:

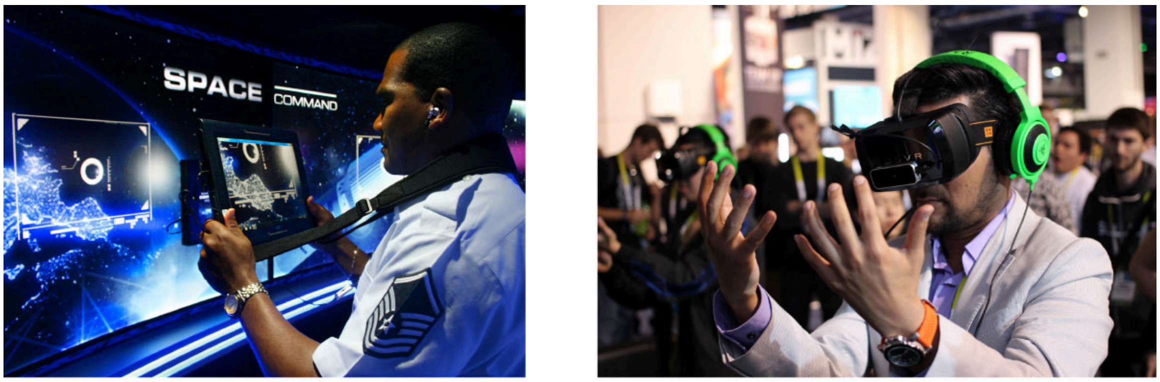
- Quantum computing harnesses quantum mechanics principles to perform complex calculations exponentially faster than traditional computers. It shows promising breakthroughs in cryptography, drug discovery, and financial modeling.
- Edge computing brings data processing closer to where data are created, reducing latency and enabling real-time applications like autonomous vehicles and smart manufacturing.
- Green computing practices focus on environmentally sustainable computing through energy-efficient hardware, smart power management, and eco-friendly data center design.

The integration of these technologies creates new possibilities. For instance, edge computing can reduce energy consumption by processing data locally, while quantum computing could optimize power grids for better energy distribution. Meanwhile, cross-platform integration allows these technologies to work together. A self-driving car might use edge computing for immediate decisions, quantum algorithms for complex route optimization, and green computing principles to maximize battery life.

If we look back over the last century, there have been many technological advancements: the automated teller machine, the hard disk drive, the magnetic stripe card, mobile telephony, desktop computers, the computer mouse, and more.

Real-World Applications of Emerging Technologies

Real-world applications of emerging technologies are boundless, and you are likely familiar with many usages. An **augmented reality (AR)** overlays digital information onto a user's environment in real time. Augmented reality often involves the use of hardware such as headsets or smartphones to overlay digital information onto physical environments. Slightly different, **virtual reality (VR)** is a computer-generated environment that simulates reality and allows users to interact with three-dimensional environments. AR and VR technologies are advancing (Figure 10.3), particularly in fields like education, health care, and entertainment. New immersive experiences are being created with better hardware, more realistic simulations, and applications in virtual collaboration.



(a) (b)

Figure 10.3 (a) Augmented reality and (b) virtual reality create immersive experiences that are being used across organizations and fields to help teach and train employees. (credit a: modification of work "Command Center Alpha" by Dale Eckroth, U.S. Air Force/Air Education and Training Command, Public Domain; credit b: modification of work "Razer OSVR Open-Source Virtual Reality for Gaming (16241057474)" by Maurizio Pesce/Wikimedia Commons, CC BY 2.0)

The biggest technological change over the last three decades has been the introduction of cell phones and smartphones, which are almost as powerful as desktop computers. In response to consumer feedback, smartphone manufacturers continue to develop and create more powerful devices with new features, improving screen size, data storage, battery life, camara quality, and processing power.

Another emerging technology, AI, is the branch of computer science focused on creating intelligent machines capable of performing tasks that typically require human intelligence, such as visual perception, speech recognition, decision-making, and language translation. While AI was originally developed in the 1950s, the power of modern computers provides new uses for AI. Artificial intelligence applications are transforming everyday business operations across industries:

- In retail, AI powers recommendation systems that suggest products based on past purchases and browsing history.
- In health care, AI assists radiologists by flagging potential abnormalities in medical images for review.
- Manufacturing plants use AI for predictive maintenance, analyzing sensor data to identify when machines might fail before they break down.
- Financial institutions employ AI to detect fraudulent transactions by spotting unusual patterns in real time.

These practical applications are examples of how AI moves beyond theory to solve real business problems. AI is not just about complex algorithms; AI is using technology to make processes more efficient, decisions more informed, and services more personalized.

LINK TO LEARNING

While AI offers many opportunities for technological advancements, it also creates challenges. For example, this documentary explores how bias is an issue in AI facial recognition (https://openstax.org/r/109FacRecogBias) and how some aspects of AI may violate civil liberties.

A type of AI called **generative AI** creates new content or ideas in the form of text, images, videos, music, audio, and other forms of data, and its supporting tools are being used to create mounds of content for different professions. Educators, students, lawyers, project managers, and even publishers are using generative AI to shorten the time on tasks. The information gathering that can be done from internet sources and web applications can be pulled together quickly through generative AI.

ETHICS IN IS

Trust Issues in Artificial Intelligence Cause Ethical Concerns

Generative AI, such as ChatGPT, will change the way we approach learning and all forms of technology. Generative AI has the ability to facilitate our learning, help with industry research, and diagnose many different problems. But, there is one major flaw—it cannot be trusted all of the time. When gathering information—such as images, audio, and text—from the internet, generative AI tools often use copyrighted material, often without obtaining permission from the intellectual property owners. While generative AI software can do a phenomenal job creating text and images, it lacks this ethical component.

Additionally, if AI is unable to find the information you request in your prompt, it may create that information itself, which can result in fake articles, photographs, events, and people. For example, following hurricanes on the East Coast during fall 2024, several fake AI-generated images were used to highlight how the hurricane affected the area.[1] In 2023, *The Guardian* determined that ChatGPT listed fake, unpublished journal articles as responses to prompts asked for through the ChatGPT interface.[2] ChatGPT may fabricate content that mimics real articles if prompted, highlighting generative AI's inability to verify factual accuracy. This is a real problem in a virtual world. If generative AI software fabricates information, how can individuals identify real information from fake information? The material generated by AI looks and reads just like real articles. This only diminishes the trust of what is found on the internet. Without any type of regulation, fake information can be referenced and even cited on the internet, leading to more misinformation and potentially disinformation.

1 "Fake Images Generated by AI Are Spreading on Social Media, Compounding Misinformation Surrounding Hurricane Recovery Efforts," ABC News, October 15, 2024, https://abcnews.go.com/US/video/fake-images-generated-ai-spreading-social-media-compounding-114824660
2 Chris Moran, "ChatGPT Is Making Up Fake Guardian Articles: Here's How We're Responding," *The Guardian*, April 6, 2023, https://www.theguardian.com/commentisfree/2023/apr/06/ai-chatgpt-guardian-technology-risks-fake-article

Quantum computing represents another real-world application of emerging technologies. Rensselaer Polytechnic Institute in Troy, New York, became the first university to house an IBM quantum computer, costing the school more than $150 million in investment capital.[3] This acquisition allows students at the college to propose research projects, and if the project has merit, time will be allotted for the project to run on the quantum computer, providing students with an opportunity to gain hands-on experience in quantum computing. In **quantum computing** computers use quantum mechanics principles to perform complex calculations exponentially faster than traditional computers. With this ability, the computer models problems and simulations that are extremely hard for researchers to conceptualize, such as complex weather forecasting, large-scale financial modeling, and advanced pharmaceutical formulas for new drugs. These and other complex problems tend to involve multiple variables that have elaborate interactions, requiring sophisticated technology to analyze and understand the problems and potential solutions. Quantum computing can provide the sophistication needed. However, the most significant challenge in quantum computing is considered to be quantum error correction; effectively managing the noise and errors that occur within quantum systems, which is crucial for achieving reliable and large-scale quantum computations.

Opportunities, Challenges, and Risks of Emerging Technologies

Emerging technologies offer a multitude of opportunities to enhance our lives in every way. For example, businesses can use AI to generate valuable data about customer experiences and satisfaction, and these data can be the impetus to make changes needed to improve customer service. Artificial intelligence can help students learn by providing educational materials like customized flash cards and quizzes. At the same time, the use of emerging technologies can pose challenges and risks that must be managed in balance with the benefits that these technologies offer.

Opportunities

Emerging technologies provide boundless opportunities for businesses to evolve and increase their competitive advantage. For example, **enterprise modeling and integration (EMI)**, a process that uses computer-based tools to model the business structure and facilitate the connection of its technology, work, and information flow across an organization, has increasingly been considered a value-add for businesses as it allows a quicker response to business challenges, and improves efficiencies. EMI connects functionality and communication between information systems to include applications, data, clouds, application programming interfaces, processes, and devices. It combines multiple integration approaches into one combined effort, with one governance model. Incorporating AI into this process would be a value-add for businesses as its capabilities can be integrated directly into products and systems to enhance performance in all system areas.

Augmented reality and VR also provide opportunities for business growth and improved performance. AR and VR technologies allow users to access animated three-dimensional experiences, videos, and targeted detection directly from their personal devices, leveraging components within the device such as the camera, magnetometer, orientation, and other functions. An example of this functionality is the use of AR-enabled applications to enhance user shopping experiences (Figure 10.4).

3 "Rensselaer Polytechnic Institute Plans to Deploy First IBM Quantum System One on a University Campus," IBM, June 28, 2023, https://newsroom.ibm.com/2023-06-28-Rensselaer-Polytechnic-Institute-Plans-to-Deploy-First-IBM-Quantum-System-One-on-a-University-Campus

Figure 10.4 Augmented reality is used with many online retailers to help shoppers visualize how that item would fit in their environment. We are now able to see how a couch fits in our living room or how a dress looks on our body prior to purchase. (credit: modification of work "Augmented reality fashion" by "sndrv"/Flickr, CC BY 2.0)

Additionally, emerging technologies continue to influence areas such as information technology, integrated manufacturing, medical informatics, digital libraries, and electronic commerce, supporting efficiencies in manufacturing, health care, e-commerce, and other facets of business. Another area impacted by emerging technologies is **information economics**, which is a branch of microeconomics that analyzes how economic decisions and consumer behaviors are influenced by knowledge and power. It focuses on how information is produced, distributed, and used in economic systems. It is an important field of study to provide businesses and other organizations with the data and knowledge they need to be competitive in the marketplace.

Another example is Bitcoin, which provides specific opportunities with its functionality, including the following:

- Data sharing between businesses is enabled in a decentralized structure where no single entity is exclusively in charge.
- Security and privacy are improved wherein transactions have end-to-end encryption protections from unauthorized activity.
- Costs are reduced as a result of efficiencies in transaction and business processes.
- Speed is increased as compared to manual processes and other technologies with similar functions.

Blockchain technology continues to evolve, finding new applications in areas like decentralized finance, supply chain management, and secure data sharing. Blockchain technologies have touted benefits and opportunities in several industries including financial institutions, health-care organizations, and nonprofit and government agencies. Customers of these industries have experienced faster and less costly clearing and settlement of financial transactions, increased security of patient privacy, and transparent supply chains to maximize social impact. Specific to health-care organizations, patient- and organizational-related benefits can be attributed to the use of blockchain technologies (Figure 10.5).

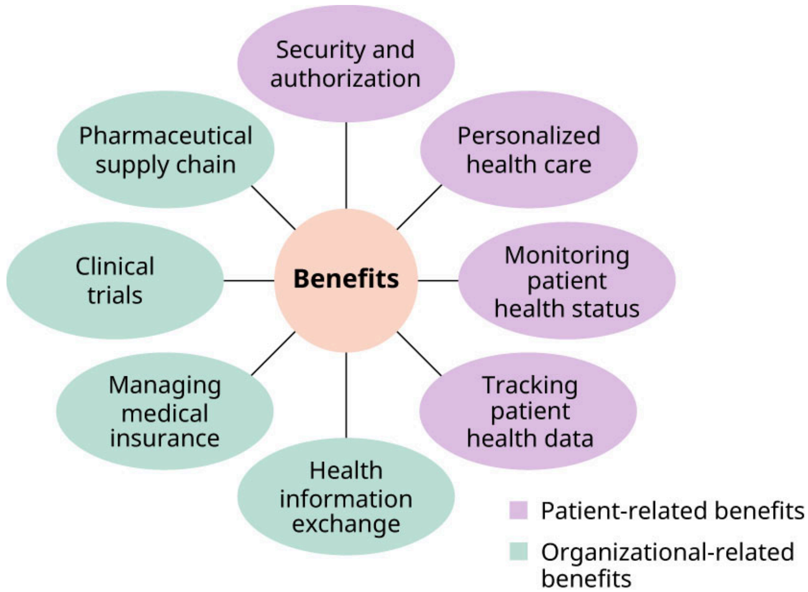


Figure 10.5 Health care's use of blockchain technology has benefits for both the health-care organization and patients. (credit: modification of work "Fig. 3. Benefits of blockchain technology" by Israa Abu-elezz, Asma Hassan, Anjanarani Nazeemudeen, Mowafa Househ, Alaa Abd-alrazaq/*International Journal of Medical Informatics*, Volume 142, October 2020, 104246. https://doi.org/10.1016/j.ijmedinf.2020.104246, CC BY 4.0)

Challenges and Risks

The opportunities derived from emerging technologies are indeed exciting; however, with their expected growth and expansion come challenges and associated risks. Security and data privacy will continue to be ongoing concerns as cybercriminals are increasingly sophisticated at usurping the security protocols of networked and cloud-based systems. Broader access to AI tools has equipped adversaries with the means to exploit these technologies, generating misleading or incorrect information. For example, in fall 2023, fake videos generated by AI featured Taylor Swift promoting Le Creuset cookware and Tom Hanks promoting a dental plan. Both celebrities decried the videos as fake content produced without their input or permission.[4]

Artificial intelligence can be used to analyze patterns and detect vulnerabilities faster than security teams can respond as the impact may be increasingly widespread as more of our services become reliant on AI. Users can be tricked into responding to impostor prompts asking for identifying information. These challenges continue to risk the security and data privacy protections needed to protect the personal information of users and customers.

There are also security and data privacy concerns with the use of AR and VR. Unauthenticated data content is sometimes used by AR browsers that facilitate the augmentation process; therefore, people can be misled by false information provided on these sites. Aside from the cybersecurity challenges, the biggest VR danger is its ability to interfere with one's visual and auditory connection to the outside world. When users are immersed in VR, they may experience a sensory conflict between what their bodies are experiencing in the real world and the visuals of the virtual world. This can lead to cybersickness, which may include disorientation, dizziness, and even nausea as users lose spatial awareness. It is crucial to maintain awareness of one's surroundings when immersed in these environments.[5]

Early implementations of blockchain technology have exposed some of the technology's challenges and risks, including ongoing threats to security and data privacy of its users. Additional challenges include the scalability and performance, interoperability, regulatory and legal concerns, and adoption and integration of blockchain technology. Energy consumption is also a significant challenge as blockchain technology requires high-powered computing equipment to create new blocks and verify transactions. The energy needs to power this

4 Megan Cerullo, "AI-Generated Ads Using Taylor Swift's Likeness Dupe Fans with Fake Le Creuset Giveaway," ed. Anne Marie Lee, CBS News, updated January 16, 2024, https://www.cbsnews.com/news/taylor-swift-le-creuset-ai-generated-ads/
5 Ann Pietrangelo, "All About Cybersickness," *Healthline*, February 4, 2021, https://www.healthline.com/health/cybersickness

equipment are so great that blockchain technology's energy consumption is causing substantial greenhouse gas emissions and contributing to climate change.

10.2 The Evolving Frontiers of Information Systems

Learning Objectives

By the end of this section, you will be able to:

- Discuss the frontiers of information systems
- Explain the convergence of information systems frontiers and emerging technologies
- Explain the opportunities and challenges related to information systems frontiers

Information systems are constantly evolving as communities of researchers, developers, think tanks, and others have expanded their thinking beyond what many of us can imagine in terms of where information systems may take us next. We have seen the evolution of systems from concept through iterations of change as the technology supporting these systems has evolved. Just look back on the evolution of the Apple iPhone, first introduced in 2007. From its initial functionalities that included mobile phone calling, personal computing, music, and a camera to its more contemporary features such as extended battery life, assistive touch, AI features, and camera resolution, iPhone functionality continues to be developed and enhanced with each new release. What do you think the next step is for the iPhone? How will the future versions of these types of technologies continue to impact our lives?

The Frontiers of Information Systems

The concept of **information systems frontiers** refers to the latest developments in the field of information systems. Frontiers explore new research areas, innovative applications, and emerging technologies that have the potential to significantly impact the field. These frontiers encompass a wide range of topics including data analytics, AI, cybersecurity, cloud computing, mobile computing, and social media.

Data Analytics

Data analytics has been identified as the future of information systems and innovation. In response to the increasing number of systems available and the breadth of data collected, organizations are increasingly looking to utilize this information. Walmart, for example, collects substantial amounts of data from their website (such as purchase histories, and products sold and returned) and in store (like customer demographics, store details, and products sold and returned). These data inform many of their business practices.

Data analytics, as you learned in Chapter 8 Data Analytics and Modeling, is the process of examining datasets to draw conclusions and insights, typically using statistical and computational methods to inform decision-making or solve problems (Figure 10.6). The insights generated from data analytics help businesses with the foundational information needed to increase performance and operational efficiencies. Along with better decision-making and operational efficiencies, data analytics can lead to the simplification of data, increasing the organization's ability to make sense of the raw data collected and share that data as needed. Refer to 8.3 Analytics to Improve Decision-Making for data analytics tools and techniques that are used to process and examine data, allowing insight into business challenges and future trends, and leading to more informed business decisions.

Figure 10.6 Data analytics uses data visualization to gain a better understanding of the habits of customers, leading to more informed decisions in business offerings and strategies. For example, Walmart might study purchase data to adjust its marketing strategy. (credit: modification of work "Examining Fisheries Data" by NOAA's National Ocean Service/Flickr, Public Domain)

CAREERS IN IS

Tech Market Researcher

Tech market research is becoming increasingly popular as organizations attempt to gauge how well technology-related products are being received. Tech market researchers study market trends, consumer behaviors, emerging technologies, competitor information, and other factors to determine the viability of a new technological product or service. It is a systematic process of gathering, analyzing, and interpreting data related to the technology sector. Specific roles in this area may include analyst, specialist, recruiter, and general researcher, with general focus in wide-ranging areas of technologies to include data cloud computing, big data management, and emerging technologies.

Artificial Intelligence

Artificial intelligence is an important innovation in information systems. Artificial intelligence is increasingly being used in many industries, including health care, logistics, manufacturing, automotive, and publishing, as well as in daily lifestyle applications. Artificial intelligence–enabled computer systems are able to process large amounts of data, identify patterns and trends, and make decisions, tasks that generally require human intelligence and a great deal of time and resources. Artificial intelligence uses reasoning, learning, problem-solving, and perception as it processes the data.

It is important to recognize that to function optimally, AI must be grounded in data that are valid and reliable. Without robust data, AI may produce inaccurate data analyses and biased algorithms. In addition, since AI doesn't have the reasoning capabilities of humans, the technology is poorly suited for situations that require adaptation to change, such as using AI to operate machinery safely.

Artificial intelligence has several subfields that focus on its different aspects

- The field of **machine learning** involves the creation of algorithms and models that enable machines to learn from or make decisions about the data without specific programming.
- A neural network is a method of AI that uses algorithms to teach computers to process data much like the human brain, using image and speech recognition.
- Deep learning uses multiple layers of neural networks to address deeper, more complex decision-making and is often considered a subset of machine learning.
- Cognitive computing simulates human thought processes via reasoning and learning.
- Computer vision teaches machines how to see and interpret information from images or videos using facial recognition, object identification, and segmentation.
- The field of **natural language processing** teaches machines to understand and generate human language and involves tasks such as speech recognition, text analysis, and language translation.

Cybersecurity

Cybersecurity is the practice of protecting internet-connected systems from internal and external threats of unauthorized access, attack, or damage to its technologies and networks. It combines the people, processes, policies, systems, and technology needed to thwart cyber risks, safeguard assets, and protect assets. Cybersecurity has become increasingly vital to business as the breadth of today's information is managed electronically. The exposure caused by a breach can compromise personal information, leading to a loss of trust and potential financial liabilities. Additionally, cybersecurity allows organizations to remain compliant with regulations, safeguard against identity theft, and protect intellectual property, finances, and people's personal information.

Currently, cybersecurity is a critical aspect of information systems, and this will continue to be true as new technologies emerge. The work of the National Institute of Standards and Technology (NIST) will continue to be important for emerging technologies. The NIST-developed Cybersecurity Framework (CSF) leads as an essential approach for organizations to create and manage their cybersecurity strategy. Refer to Chapter 5 Information Systems Security Risk Management and Chapter 6 Enterprise Security, Data Privacy, and Risk Management for more on information on cybersecurity.

As new technologies emerge, there remain several pivotal layers of cybersecurity necessary to guard against ever-evolving cyber threats:

- Application security is a principal component of cybersecurity, adding security inside an application to shield it from attacks on vulnerabilities within its code. Various tools (such as firewalls, antivirus software, encryption techniques, and web application firewalls) combined with various types of application security (authentication, authorization, encryption, logging, and application security testing) assist in keeping applications secure.
- Companies must protect customer, client, employee, and user information from unapproved access, use, modification, loss or deletion. This component is dedicated to protecting the integrity of the data residing within a system.
- Network security protects the network from unapproved access and potential dangers. Firewalls and antivirus software are examples of strategies used to support network security efforts.
- Disaster recovery planning helps businesses identify the necessary and mission-critical applications vital to maintain the operations of the organization and how the implementation of these plans will occur in the event of a cyberattack.
- Operational security encourages management to step inside the role of a hacker to identify areas of vulnerability within the organization.
- End-user security targets the safeguards of individual devices connected to a network, such as computers, tablets, printers, and smartphones. Coupled with end-user education and training, these controls help to alleviate security threats that may be caused by human error.

Biometrics are increasingly used to authenticate a person's identity, such as fingerprints to access smartphones, or the use of facial recognition technology at airport smart-gates. Some examples of biometrics that could be used in 5G network security include fingerprint scanning, iris recognition, and voice recognition.

Cloud Computing

Cloud computing is an emerging technology defined as the use of hosted services like data storage, servers, databases, networking, and software that run over the internet (or an intranet) rather than on private servers and hard drives. Cloud computing services are available via public, private, or hybrid means and are generally owned by a third party, allowing the customer to pay for the choice of how they want their infrastructure to be managed and supported. Review Chapter 7 Cloud Computing and Managing the Cloud Infrastructure for more information on cloud computing.

CAREERS IN IS

Cloud Engineering

Cloud engineers are increasingly needed to support the design, development, maintenance, security, and management of cloud infrastructures. Cloud engineers ensure the security of the network. Additionally, they assist with the planning and design of cloud computing applications and services for the business, deployment of cloud-based infrastructure, and programming code in various languages such as Java, Python, and C++. They also work with organizations on disaster planning, preparedness, and recovery. Experience working with coding languages, as a systems administrator or network engineer and excellent written and communication skills are necessary to succeed in this position.

Mobile Computing

The emerging technology of **mobile computing** involves the strategies, technologies, products and services that enable users to access information without restricting the user to a single geographic location. Combined, mobile computing technologies support the use of mobile devices that are portable, and wireless devices that are enabled to transmit data, voice, and video communications. The convenience of mobile computing allows people to access network services anywhere and anytime. Most could not have imagined a few decades ago a future where you could call or text a relative in another country from an underground subway train or connect with a long-lost classmate through a social media application.

Mobile computing combines infrastructure (technical pieces that enable communication such as a wireless network), hardware (physical devices such as laptops), and software (applications and operating systems) technologies. Characteristics of mobile computing technologies include portability, connectivity, social interactivity, context sensitivity, and individualization. These are all applicable to the types of mobile devices consumers enjoy using, such as tablets, mobile phones, and laptop computers.

In addition to being able to privately connect, interact, and collaborate with people through different applications, there are several other advantages to mobile computing. For example, studies have shown that mobile computing increases productivity. With the move toward working remotely, organizations have realized that the cost of an office location may not make sense when employees can work from any location and be just as productive.[6] Mobile computing has also enabled a plethora of entertainment options with applications that provide movies (like Netflix and YouTube), games (such as Wordle), lifestyle content (for example, HGTV and Amazon), and more. Additionally, mobile computing now supports and connects to the cloud and cloud computing services, allowing data such as photos, videos, and documents to be secured for future retrieval.

Mobile computing does have limitations. For example, the range and bandwidth (the capacity at which a network can transmit data) of some devices is limited, leading to transmission interference or unwanted disruptions while communicating. This can severely interrupt the quality of the sound or picture being displayed on the device. Security standards that govern mobile computing technologies also remain an issue as the industry regulations can lag behind the rate of innovation. Additionally, mobile computing technologies present power consumption and battery charging challenges. For example, batteries can be negatively impacted by temperature changes, making it difficult to recharge and maintain battery performance.

The Convergence of Information Systems Frontiers and Emerging Technologies

In the context of computing and technology, **convergence** is the joining of two or more different entities in a single device or system. The convergence of emerging technologies and IS frontiers can create new

6 Jane Thier, “Bosses, You’re Wrong: Remote Workers Are More Productive than Your In-Office Employees,” *Fortune*, October 20, 2022, https://fortune.com/2022/10/20/remote-hybrid-workers-are-more-productive-slack-future-forum/

opportunities for innovation and growth as the research and development processes in new frontiers helps foster and promote emerging technologies to develop and evolve. For example, the convergence of AI and data analytics can help organizations make better decisions by analyzing vast amounts of data in real time. It can enable organizations to gain a competitive edge, optimize operations, and drive business value by providing insights into data that a data analyst may not be able to uncover. Data analysts will still be needed to interpret the data in a business sense as these technologies do not yet have the capacity to accomplish such tasks.

The IoT can connect devices and sensors to create smart systems that can optimize operations and enhance user experiences. These technologies can be leveraged to create smart homes, where internet-enabled appliances and devices can be managed remotely via a connected network. For example, IoT smart devices can support the needs of people who are hard of hearing or deaf by providing real-time alerts, such as a smoke detector that activates non-sound-based alarms. Overall, the intersection of emerging technologies and IS frontiers is an exciting area that has the potential to transform various industries and improve people's lives.

Opportunities, Challenges, and Risks of Information Systems Frontiers

The rapidly evolving field of information systems presents both significant opportunities and complex challenges for organizations navigating the digital landscape. Frontiers of information systems, such as data analytics, AI, cloud computing, mobile computing, and social media, provide opportunities, challenges, and even risks to people and organizations as they continue to evolve.

Opportunities

Businesses can expect IS frontiers to expand and grow, becoming more advanced and mature in their functions. For example, natural language processing enhancements will further the abilities of machines to understand and generate human language, making it easier for users to interact with information systems. This expected growth may provide increased employment opportunities to develop and manage such systems, as well as a growth in educational and training opportunities in these areas.

Another opportunity afforded by these systems will be an overall improvement in networking infrastructure, allowing increased compatibility between networked systems. Problems with voice, data, and image transmission will be reduced, improving overall communication quality and delivery. This will also lead to a reduction in hardware and software costs, reducing the overall costs of processing data. Over time, the cost savings should make information systems more affordable, allowing businesses to become more competitive.

We have already seen exponential growth in mobile computing in the variations of devices, their functionality, and their processing power. Mobile computing will continue to exhibit improved functioning, making it easier to use and maintain, and possibly become more affordable in the future.

Challenges and Risks

Data analytics will experience challenges with big data (large amounts of complex data) in that it is unable to be stored, processed, or analyzed in traditional data storage formats—a significant challenge. However, analyzing this data in a timely manner can help decrease risks to society, nature, or the ecosystem. For example, hospitals, pharmaceutical companies, and other medical and health organizations store large amounts of medical data. When completed in a timely manner, data analytics can provide trend analysis and identify potential health-related threats to different communities, improving and even saving lives. Another risk occurs when, even if data are analyzed in a timely manner, the analysis uses bad data, such as those caused by outdated records, inaccurate data integration processes, and data entry errors.

Data breaches are an increasing concern as hackers are becoming more sophisticated in breaking through networks. In health care, which shows much promise in the convergence of IS frontiers and emerging technologies, 45.9 million U.S. health-care records were breached in 2021, 51.9 million breaches occurred in 2022, and this increased to 133 million records exposed, stolen, or otherwise impermissibly disclosed in 2023.[7] Care needs to be taken to protect data as it is processed in new ways.

Businesses are also challenged to maintain regulatory compliance as the increased use of these technologies continues to push the boundaries of regulatory bodies. It is becoming more difficult and expensive to ensure adherence to these regulations, and violations may result in substantial penalties, data breaches, and reputational risk to the business.

Challenges and risks for cloud computing include misconfiguration of security settings, a common vulnerability that occurs when security settings such as default configurations, improper access controls, insufficient firewall protections, and other misconfigurations result in security issues. The data itself may pose quality issues where duplicate data, corrupt data due to human error, or mixed data types may exist, all creating challenges when gathering data for analysis.

LINK TO LEARNING

The publication *Information Systems Frontiers: A Journal of Research and Innovation* (https://openstax.org/r/109ISFrontiers) explores topics in areas of emerging technologies, including research developments in EMI, medical informatics, mobile computing, and e-commerce.

10.3 Societal and Global Importance of Emerging Technologies in Information Systems

Learning Objectives

By the end of this section, you will be able to:

- Identify the societal and global impact of emerging technologies
- Describe the global reach of research and innovation
- Examine how research and innovation lead to emerging technologies
- Discuss questions in emerging technologies

Emerging technologies are changing how information systems–related work and projects are managed. Virtual assistants and chatbots, machine learning, predictive analyses, resource optimization, natural language processing, data management, and other functionalities of emerging technologies help to automate repetitive and routine tasks, enhance collaboration with team members and stakeholders, and efficiently plan and track project tasks.[8] Societal innovation can also have a major impact on social groups, resulting in a change in behavior or practice that has far-reaching consequences worldwide. In an era defined by rapid technological advancement, the emergence of innovative technologies has revolutionized societal interactions.

7 Steve Alder, "Healthcare Data Breach Statistics," *The HIPAA Journal*, January 15, 2025, https://www.hipaajournal.com/healthcare-data-breach-statistics/
8 Ana María Choquehuanca-Sánchez, Keiko Donna Kuzimoto-Saldaña, Jhonatan Rubén Muñoz-Huanca, et al., "Emerging Technologies in Information Systems Project Management," *EAI Endorsed Transactions on Scalable Information Systems* 11, no. 4 (2024), https://doi.org/10.4108/eetsis.4632

Societal and Global Impact of Emerging Technologies

The societal and global impact of emerging technologies refers to their worldwide effect of change—to economy, culture, public policy, public services, health, the environment, and quality of life. For example, emerging technologies are rapidly changing many aspects of the finance industry. When customers contact their financial institutions with general banking questions, such as location, hours, account balance, and bill payments, they can interact with AI-enabled systems to get the information they need and accomplish banking tasks. Other uses include fraud detection, anti-money-laundering, risk management, credit scoring, and trade and investment services (Figure 10.7). By automating routine tasks, organizational resources (human and financial) can be allocated elsewhere, improving efficiency. As noted during a 2023 panel discussion at the JP Morgan NBFI Leaders Forum in Sydney, Australia, generative AI could add $2.4 to $4.4 trillion annually to the global economy.[9] It is expected to impact 75 percent of areas, such as customer operations, marketing, software engineering, and research and development, while reducing fraud and account rejection rates by 15 to 20 percent.[10] We can also look at these services, enabled by AI and other emerging technologies, as contributors to the closure of over 3,000 branches of large financial institutions in 2023 due to the rise of digital banking.[11]

Figure 10.7 The financial sector utilizes artificial intelligence to support many areas of its business. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Another emerging technology with a societal impact is **self checkout (SCO)**, in which machines are enabled with artificial intelligence technology, product images, barcodes, and other mechanisms for customers to complete purchases. First introduced in the 1980s, SCO technology began appearing in stores in greater numbers in the 1990s. The SCO systems market generated $3.5 billion in revenue in 2021 and is expected to grow 13 percent between 2022 and 2028 (Figure 10.8).[12]

9 Michael Chui, Roger Roberts, Lareina Yee, et al., *The Economic Potential of Generative AI: The Next Productivity Frontier*, (McKinsey & Company, June 14, 2023), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction
10 "How AI Will Make Payments More Efficient and Reduce Fraud," J.P.Morgan, November 20, 2023. https://www.jpmorgan.com/insights/payments/payments-optimization/ai-payments-efficiency-fraud-reduction
11 Courtney Rau and Konner McIntire, "Fact Check Team: Major Banks Close Their Doors amid Rise in Digital Banking," The National News Desk, November 28, 2023, https://thenationaldesk.com/news/fact-check-team/fact-check-team-major-banks-close-their-doors-amid-rise-in-digital-banking-pnc-jpmorgan-chase-bank-of-america-citizens-federal-deposit-apps-websites-branches-locations
12 "Global Self-Checkout Systems Market Size, Share, Trends, Industry Growth by Component (Systems, Services), by Type (Cash, Cashless), by Application (Retail, Financial Services, Entertainment, Travel, Healthcare, Others), by Region, and Forecast to 2028," Research Corridor, updated March 6, 2024, https://www.researchcorridor.com/self-checkout-systems-market/

Figure 10.8 Self-checkout systems, which rely on artificial intelligence technology, enable customers to independently complete purchases. (credit: "Self Checkout" by "pin add"/Flickr, CC BY 2.0)

LINK TO LEARNING

The processes of [self-checkout technology (https://openstax.org/r/109SelfCheckout)](https://openstax.org/r/109SelfCheckout) have encountered unexpected challenges, including scanning difficulties, inaccuracy of produce scales, problems with weights in bagging areas, missed scans, and theft, to name a few. This technology can be costly to a business with a four-kiosk system, costing six figures, on average. Some organizations are reversing the course on this technology by putting limits on its use, installing cameras, and even removing systems.

The societal and global impact of emerging technology may not be apparent right away. For example, social media began in the 1990s with small platforms like Classmates.com, GeoCities.com, and SixDegrees.com, all with messaging and chat functions. Today, billions of people worldwide use social media daily for purposes including finding entertainment, interacting with others, and conducting business. Social media has expanded beyond its original designs to include e-commerce functions that allow users to buy, sell, or trade items, earn income, and find other financial incentives for use. Businesses often utilize e-commerce functions to run targeted ads, build brand awareness, generate online sales, and attract a global online following. The interaction of businesses in real time can foster a sense of community and loyalty.

Another example is the availability and adoption of solar power by consumers. First introduced in the 1980s, solar power has experienced significant growth as a result of improved solar energy technology. The conversion of energy from the sun into power for electricity and heat, or solar power, is generated through the use of solar panels. These can be found for general use on private rooftops or solar farms/fields, and large areas of land with interconnected solar panels generate large amounts of energy at the same time.

The advancements in solar power technology along with federal incentives and tax credits in the United States have increased sales of solar cells. Over five million solar systems have been installed with enough solar energy-generating systems installed to power 32.5 million homes (Figure 10.9).[13] In other parts of the world, solar technology is being adopted in places where laws have been passed to enable access of solar energy to their citizens. The adoption and widespread use of this emerging technology have helped consumers lower electricity bills, increase property values, and reduce dependence on fossil fuels, all positive impacts on public health and the environment.

Figure 10.9 Solar farms, such as the one shown here, use solar panels to convert energy from the sun into power used to support electricity and provide heat. (credit: “Hawaii solar; a photovoltaic power station” by Reegan Moen, U.S. Department of Energy/ Wikimedia Commons, Public Domain)

While there are positive societal and global impacts of emerging technology, such as job creation, improved access to education and health care, and environmental conservation efforts, there can also be negative consequences. Unintended consequences of emerging technology include increased inequality, job loss, and a harmful impact on the environment. For example, using AI may be challenging for individuals with different abilities, reducing the opportunity for them to interact with AI-enabled systems. Similarly, solar power technologies are limited to those who have the financial means to invest.

LINK TO LEARNING

Read this article from *Forbes* to learn how AI can exploit consumer vulnerabilities (https://openstax.org/r/109EthicsAI) if not built and trained ethically, especially in the marketing industry.

The global impact of emerging technologies is also evident across frontiers in information systems. Data analytics tools and techniques are being used and applied in all aspects of society from transportation to health care, marketing to education, finance to political campaigns. Public health organizations collect nonidentifying information on disease prevalence to spur and fund research efforts, provide targeted medicines, improve efficiencies in health care–related supply chains and logistics, resource health care, and initiate targeted marketing campaigns aimed at increasing awareness and disease prevention. The year-by-year identification of different strains of flu and its prevalence is an example of how data analytics can drive

13 "5 Millions Solar Installations: Powering American Communities," Solar Energy Industries Association, updated May 2024, https://seia.org/5m/

societal and global change.

We also see the societal and global impacts of data analytics in the frontier of education. A student's personal learning experience is enhanced, educational resources are optimized, and the student's strengths and weaknesses are identified in order to tailor instruction and set them up for success. The same transformative effects can be seen in environmental conservation efforts where deforestation, pollution, and climate change data are collected and used to enact positive change. This is evident, for example, in the World Resources Institute's work on global forestry, where analytics is helping to identify deforestation in countries across the world, improving impacts to climate, biodiversity, and human well-being.[14]

The Global Community of Research and Innovation

Without research and development, we would not have smartphones, computers, the internet, or any of the technologies many of us use on a daily basis. Research and development are crucial in ensuring that technology continues to evolve and improve, and that new and innovative solutions are developed to address emerging challenges.

The global community of scientists supporting research and innovation continues to make strides toward furthering new findings, technologies, and processes. And those latest developments in the field of information systems continue to push to further the potential reach of new technologies worldwide. For example, global growth in data analytics and the predictive analytics market is expected to grow from $16.41 billion in 2023 to $83.98 billion by 2032.[15]

Regionally, North America is leading global efforts in data analytics and the predictive analytics market, and the largest increases in growth are in Europe, Asia-Pacific, Middle East and Africa, and South America.[16] Together, countries in these regions are increasingly seeing solution and service gains in banking, financial services, insurance, health care, telecommunications, and information technology. For example, the banking industry is using these technologies to customize insurance plans and premium amounts based on user data and documentation. Large global organizations will dominate these markets as they have increased their capacity to store, process, and analyze large amounts of data to leverage the outcomes and create marketing strategies that target customers and improve user experiences.

We can also find global communities working to adopt and expand on these technologies in uses like the continued adoption and development of 5G. This fifth-generation wireless technology is an example of how mobile computing is evolving regionally and throughout the world, increasing the speed of use, enhancing connectivity, and enabling other mobile options while connected. The next generation, 6G technology is currently being developed in regions throughout the world and is expected to be available in the United States in 2030.[17]

How Research and Innovation Lead to Emerging Technologies

Research and innovation have played a significant role in the growth of emerging technologies. Research, or the systematic process to generate understanding or knowledge, is a precursor to innovation, the process of using the knowledge generated from research to meet real needs. When we think of research, we might imagine a scientist behind a microscope. But research can be thought of more broadly, beginning with a broad idea, leading to preliminary investigation, designing and planning, collecting and interpreting data, and then disseminating findings.

14 Mikaela Weisse, Elizabeth Goldman, and Sarah Carter, "Forest Pulse: The Latest on the World's Forests," *World Resources Institute*, updated April 4, 2024, https://research.wri.org/gfr/latest-analysis-deforestation-trends
15 *Global Market Overview and Competitive Analysis* (Introspective Market Research, May 2024), https://introspectivemarketresearch.com/reports/data-science-and-predictive-analytics-market/
16 *Global Market Overview and Competitive Analysis* (Introspective Market Research, May 2024) https://introspectivemarketresearch.com/reports/data-science-and-predictive-analytics-market/
17 "ITU's IMT-2030 Vision: Navigating Towards 6G in the Americas," 5G Americas, September 2024, https://www.5gamericas.org/itus-imt-2030-vision-navigating-towards-6g-in-the-americas/

Innovation is a catalyst for change as stagnation or inactivity can impede the growth of a competitive and fiscally sound organization. The innovation process is generally composed of three systematic steps: conception, implementation, and marketing (Figure 10.10). It begins with a conceptual idea—its evaluation, the generation of requirements, and the planning needed for potential implementation. The implementation stage is where the idea is further developed or constructed, and a prototype or pilot is produced and tested. Generally, within the marketing step, the prototype or pilot application is moved to production or to launch for use. The organization may also choose specific markets to release the product.

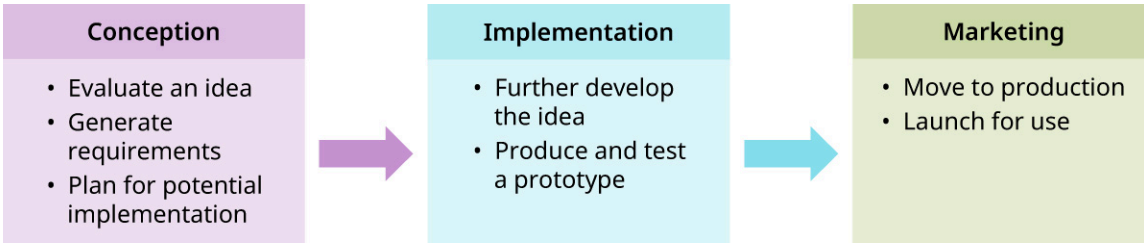


Figure 10.10 Innovation can occur in three steps: conception, implementation, and marketing. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

FUTURE TECHNOLOGY

Agricultural Technologies

The agricultural industry continues to make research and innovation gains in addressing food insecurity, animal welfare, the environmental impacts of meat production, and the overall protection of human health. Research and innovation advances in tissue engineering techniques and regenerative medicine technologies have led to the production of cultured or cultivated meat, produced from culturing animal cells in vitro. These advances represent new and innovative approaches that significantly enhance the efficiency, productivity, and sustainability of farming practices as they integrate digital tools, sustainable practices such as drone monitoring, precision agriculture using GPS, and automation and robotics. *New Harvest*, a leading U.S.-based nonprofit research organization, is pioneering these emerging technologies with the goal of reducing dependence on animal agriculture by using cells instead of animals.[18]

Through its continuous research and innovation processes, India has become a global leader in information technology and **business process outsourcing (BPO)**, a service industry that supports outsourcing of business service operations to third-party vendors. It is estimated that these services have garnered $157 billion in the fiscal year 2021–22, comprising $106 billion of information technology services and $51 billion of BPO services, respectively.[19] This growth has also contributed to the emergence of an Indian workforce trained to solve complex problems and manage the technical functions of global corporations including consulting, design, product development, business process management, and infrastructure support.

Governments, think tanks, and private enterprises have also made major contributions to the research of new discoveries and uses for emerging technologies. The U.S. government has contributed to research and innovation through its support of federally funded agencies, such as the Department of Defense, the National Science Foundation, National Aeronautics and Space Administration (NASA), and the Environmental Protection Agency Office of Research and Development. According to the National Science Board, the proposed fiscal year 2025 budget for federal research and development is approximately $201.9 billion, with the Department of Defense (DOD) accounting for 46 percent and the Department of Health and Human Services accounting for 25 percent.[20]

18 "New Harvest Is a Field-Building Organization Advancing Cellular Agriculture Globally," New Harvest, accessed December 19, 2024, https://new-harvest.org/

19 "How India Is Emerging as the World's Technology and Services Hub," EY India, January 27, 2023, https://www.ey.com/en_in/india-at-100/how-india-is-emerging-as-the-world-s-technology-and-services-hub

The RAND Corporation, considered one of the top think tanks in the world, is an example of an organization or institution that maintains a scholarly and interdisciplinary approach to research on particular issues, policies, or ideas. The RAND Corporation receives public and private funds to support research efforts, educational opportunities, analyses, consulting, training, and other services, with $390 million in revenue in 2023.[21] Areas of expertise include public policy, education, environment, national security, law, and corporate governance, and also science, technology, infrastructure, defense, and economic development.

Questions in Emerging Technologies

While there is an emphasis on a multidisciplinary approach for emerging technologies in information systems that draws from such fields as computer science, telecommunications, operations research, economics, and cognitive sciences, the field is constantly evolving, and there are many questions to explore. Here are some of the central issues.

How can we ensure the ethical and responsible use of emerging technologies such as AI, blockchain, and the IoT? Ensuring the ethical and responsible use of emerging technologies should occur at individual and organizational levels as there is a great deal at stake. As complex technologies are developed, it is necessary to consider bias, fairness, transparency, privacy, and data protection as well as the human control of these technologies. Additional proactive ethical strategies to consider include the following:

- Promote open and transparent dialogue among technical teams, users, leadership, and other stakeholders about the ethical implications needed to navigate the complex landscape that technologies may bring.
- Foster collaboration and engage diverse stakeholder perspectives to create, adopt, and promote ethical standards.
- Embed ethics within the design through all stages from conception to implementation. Be sure to address questions in the integration to cover processes in place, levels of access, responsible parties or departments to respond, and ongoing monitoring processes.
- Invest in research and education of emerging technologies to aid in the development of ethical guidelines.

How can we design information systems that are resilient to cyberattacks and other security threats? As new technologies and attack vectors emerge, how can we keep systems and data safe? Organizations have recognized the need to design information systems that are resilient to cyberattacks and other security threats. Creating cyber-resilient strategies is key to safeguarding systems and data, such as the following best practices:

- Identify emerging trends in cybersecurity. Explore the specific technology and the threats that may be inherent in them. Discuss the challenges posed for each, the potential controls, validating techniques and other means to manage their vulnerabilities with leadership and other stakeholders.
- Build a resilient infrastructure. Be sure to build a comprehensive cybersecurity infrastructure that includes all the hardware, software, firewalls, encryption protocols, and regular security surveillance needed to mitigate potential risks.
- Collaborate with external partners. Explore collaborative communities to include vendors, industry peers, and governing organizations. The value of partnerships with external partners may far outweigh the cost of an attack.
- Explore the cybersecurity landscape. Research the evolving nature of threats, methods to address them, and potential impacts to the organization, such as regulatory penalties, financial losses, reputational damage, and the loss of customer trust.
- Implement training and security protocols within the organization to include user controls, privileges, and data access. Multifactor authentication and regular access reviews can also aid in strengthening security.

20 *Laurie Harris, Lisa S. Benson, Marcy E. Gallo, et al., Federal Research and Development (R&D) Funding: FY2025* (Congressional Research Service, December 9, 2024), https://crsreports.congress.gov/product/pdf/R/R48307/2
21 *2023 RAND Annual Report* (RAND Corporation, April 10, 2024) 39, https://www.rand.org/pubs/corporate_pubs/CPA1065-4.html

- Develop an incident response plan. Creating a culture of prompt incident reporting to test the effectiveness of systems is needed to identify areas of improvement.

How can we leverage emerging technologies to improve health-care delivery and patient outcomes? For example, can AI be used to diagnose diseases more accurately or predict patient outcomes more effectively? Emerging technologies are increasingly used throughout the health-care sector to improve health-care delivery and patient outcomes. According to the Health Information and Management Systems Society, a leading organization driving reformation of health-care delivery through information and technology, health-care stakeholders are optimistic about emerging health-care-related tools and technologies and their ability to improve accuracy and efficiency in care.[22] Another study found that 80 percent of 80 percent of health organizations intend to expand their use of digital systems between 2022 and 2027.[23] Figure 10.11 shows some of these emerging technologies and some examples of how they are being used to support health-care delivery:

- Artificial intelligence has been leveraged in areas such as clinical decision support where presenting conditions can be narrowed down to further identify a diagnosis or causation of a presenting health challenge. It can also improve the accuracy of the diagnosis using predictive analyses and other functionality. Additionally, AI has been used to support standard operating procedures, ensuring that patient care protocols are consistently adhered to.
- Cloud computing has enabled health-care organizations to expand their capacity for data storage and scalability. Cloud computing–enabled interoperability in devices supports collaboration and data-sharing capabilities between patients and their care team.
- The management and secure transfer of patient medical records through hospitals, pharmacies, diagnostic laboratories, and other health-care entities have been attributed to the use of blockchain technologies. Its system also enables increased protection and safeguards of health-care data.
- The IoT enhances patient monitoring capabilities, medication adherence, and overall well-being. IoT-enabled devices support videoconferencing, allowing patients to confer with their medical team remotely. These devices also support the distribution of medical information where patients can use their mobile devices to track health measures or check the results of medical tests.

22 “Future of Healthcare Report: Exploring Healthcare Stakeholders’ Expectations for the Next Chapter,” *HIMSS*, August 11, 2021, https://www.himss.org/resources/future-healthcare-report-exploring-healthcare-stakeholders-expectations-next-chapter
23 Bill Siwicki, “Where to Invest Increasing Digital Health Dollars,” Healthcare IT News, August 24, 2022, https://www.healthcareitnews.com/news/where-invest-increasing-digital-health-dollars

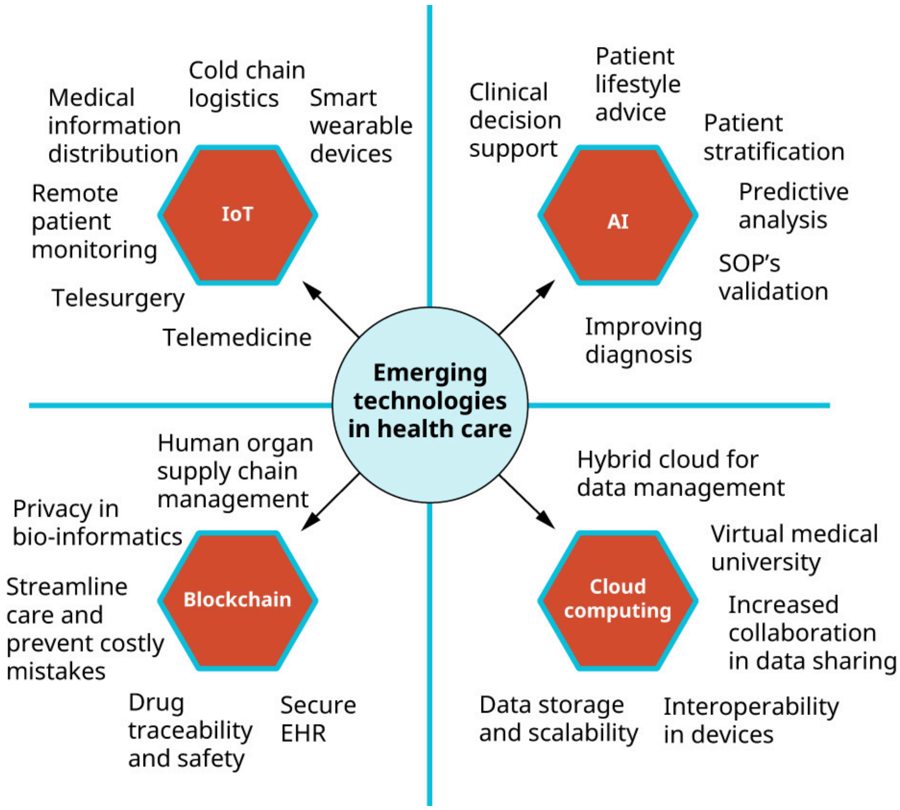


Figure 10.11 Emerging technologies support several segments of health-care delivery to include clinical integration and operational optimization. (credit: modification of work "Figure 2" by Abdulatif Alabdulatif, Ibrahim Khalil, and Mohammad Saidur Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis," *Applied Sciences* 12, no. 21 (October 31, 2022): 11039, https://doi.org/10.3390/app122111039, CC BY 4.0)

What are the implications of emerging technologies for the future of work? How will automation and AI impact the job market, and how can we prepare workers for this new reality? There are some who believe that emerging technologies will take away jobs. A more optimistic viewpoint explores the potential these technologies will have to not only enhance and transform the skills and competencies of the current workforce but also add new types of roles to augment existing roles. For example, traditional sales jobs (cold-calling, door-to-door) may have decreased due to the introduction and use of new technologies; however, new opportunities have been created and leveraged for companies to hit their sales targets. For example, automating sales activities can increase efficiencies such as lead qualification and generation, the use of virtual assistants to manage human tasks more efficiently, and algorithms to identify promising prospects. Data analytics can also create algorithms to identify opportunities and customer-focused prospects. Additionally, social media provides marketing options, reducing the need for cold-calling, improving the reach of services, and increasing the potential to attain sales goals. According to the *Harvard Business Review*, there are several capabilities companies need to have or build to realize the value of AI to exceed its costs.[24] They recommend that companies change behaviors to maximize learning, control experimentation to determine the value of a potential full organizational rollout, measure the value of the technology for the business, manage the data as current data stores may need to be augmented to support the potential volume of data captured, and develop personnel to engage with the technology to improve productivity and operations.

24 Tom Davenport and John J. Sviokla, "The 6 Disciplines Companies Need to Get the Most Out of Gen AI," *Harvard Business Review*, July 8, 2024, https://hbr.org/2024/07/the-6-disciplines-companies-need-to-get-the-most-out-of-gen-ai

How can we ensure that emerging technologies are accessible to all, regardless of income, location, or ability? How can we bridge the digital divide and ensure that everyone has equal access to the benefits of new technologies? The adoption of responsible and inclusive approaches is necessary to ensure inclusivity and accessibility of emerging technologies. According to the World Health Organization, an estimated 1.3 billion people, or 16 percent of the global population, experience significant physical and/or mental disabilities.[25] Best practices for inclusive and accessible design include conducting user research, engaging diverse perspectives, prioritizing features, and creating flexible designs that are tested and iterated. We must bridge the gap between the technological world and users to increase accessibility. Some technologies have been developed with accessibility challenges in mind, such as GPT-4 offering advanced capabilities such as visual assistance to those who are visually impaired. Apple has introduced a wide range of tools to improve voice-controlled and assistive technology functions within its devices. Additionally, Google has improved its navigation features within Google Maps so users can access wheelchair accessibility, walking routes, and live experiences for those with visual impairments.

As emerging technologies continue to evolve, research and development will continue to address new issues and ensure that technology advances and meets society's needs. An important part of this will be addressing the power demands of AI and other emerging technologies. To ensure that organizations have sufficient resources to support these power needs, research and development need to focus on sustainable energy practices. This may include efforts such as the development of processors that are more energy efficient and collaboration on open sources to share power. Efforts to manage the power consumption of emerging technologies can reduce these technologies' environmental footprints as well as improve efficiencies and cost-effectiveness.

ETHICS IN IS

Ethics in the United Kingdom

There are growing calls for ethics in research and innovation, particularly as emerging technologies are increasing their global reach and impact. The UK Research and Innovation organization is one such entity that has acknowledged the need for collective responsibility where funders, researchers, stakeholders, and the public all have a role to play. The organization says that the responsibility goes beyond the consideration of risk and regulation and should also be aligned with creating value for society in an ethical and responsible way. The Framework for Responsible Research and Innovation was created as a guiding process to promote creativity and opportunity for science and innovation.[26]

25 "Disability," World Health Organization, March 7, 2023, https://www.who.int/news-room/fact-sheets/detail/disability-and-health
26 "Framework for Responsible Research and Innovation," UK Research and Innovation, updated March 16, 2023, https://www.ukri.org/who-we-are/epsrc/our-policies-and-standards/framework-for-responsible-innovation/

Key Terms

augmented reality (AR) technology that overlays digital information onto a user's environment in real time
blockchain shared, immutable ledger that facilitates the process of recording transactions and tracking assets
business process outsourcing (BPO) service industry that supports outsourcing business service operations to third-party vendors
convergence joining of two or more different entities; in the context of computing and technology, into a single device or system
cryptography process of hiding or coding information so that only the intended recipient can read it
emerging technology software or hardware that enhances the user experience by obtaining or using information and data in new and exciting ways; can be used to describe new technologies or the continuing development of existing technologies
enterprise modeling and integration (EMI) process that uses computer-based tools to model the business structure and facilitate the connection of its technology, work, and information flow across an organization
generative AI type of artificial intelligence that creates new content or ideas in the form of text, images, videos, music, audio, and other forms of data
information economics branch of microeconomics that analyzes how economic decisions and consumer behaviors are influenced by knowledge and power
information systems frontiers latest developments in the field of information systems, exploring new research areas, innovative applications, and emerging technologies that have the potential to significantly impact the field
machine learning use of algorithms and models that enable machines to learn from or make decisions about data without specific programming
mobile computing strategies, technologies, products, and services that enable users to access information without restricting the user to a single geographic location
natural language processing teaching machines to understand and generate human language; involves tasks such as speech recognition, text analysis, and language translation to build this understanding
quantum computing use of quantum mechanics principles to perform complex calculations exponentially faster than traditional computers
robotics branch of engineering and computer science that involves the conception, design, building, and operation of robots, creating intelligent machines that can assist humans with a variety of tasks
self checkout (SCO) machines enabled with artificial intelligence technology, product images, barcodes, and other mechanisms for customers to complete purchases
virtual reality (VR) computer-generated environments that simulate reality and allow users to interact with three-dimensional environments

Summary

10.1 Defining Emerging Technologies

- Emerging technology is defined as software or hardware that enhances the user experience by obtaining or using information and data in new and compelling ways. It includes novel technologies and the continuing development of existing technologies.
- Emerging technology can be found in many areas including education, information technology, and AI, and continues to have great potential to provide synergies with other technologies of similar or different functionalities.
- Characteristics of an emerging technology include its novelty or newness, rapid advancement, and disruptive potential.
- Emerging technologies may be developed from a combination of private and/or public entities, such as government agencies and educational institutions.

- Blockchain, AI, AR, and VR are all real-world applications of emerging technologies.
- Opportunities, challenges, and risks are apparent with these technologies and should be considered for each technology.

10.2 The Evolving Frontiers of Information Systems

- Frontiers of information systems are the latest developments in the field of information systems.
- IS frontiers explore new research areas, innovative applications, and emerging technologies that have the potential to significantly impact the field.
- The convergence of IS frontiers and emerging technologies provides opportunities for two or more of these technologies, like AI and data analytics, to converge, which can help organizations analyze vast amounts of data in real time and inform decision-making.
- The opportunities, challenges, and risks associated with these information systems continue to evolve as they are further integrated for business and personal use.

10.3 Societal and Global Importance of Emerging Technologies in Information Systems

- Emerging technologies can have far-reaching societal and global consequences.
- The emergence of innovative technologies, such as AI-enabled customer service systems in banking, SCO machines, e-commerce-enabled websites, and solar power, has revolutionized societal interactions and affected worldwide change in economy, culture, public policy, public services, health, and the environment.
- Data analytics tools and techniques are being applied in all aspects of society, helping organizations to leverage their functionality to support business processes.
- Emerging technologies and innovations are expected to continue to grow globally to include data analytics, IoT, and others, with solution and service gains in the banking, financial services, and insurance sector, health care, telecommunications, and information technology.
- Research is a precursor to innovation, and it begins with a broad idea and ends with the dissemination of findings. The idea, or concept, evolves through specific process steps to where it will be available for market use.
- Emerging technologies will continue to evolve and so will be of great importance in research and development. As the field continues to evolve, new questions will arise, and researchers will need to work together to find answers.

Review Questions

1. Which of the following statements about emerging technologies is false?
   - **a.** Emerging technologies only include hardware.
   - **b.** They can be described by their novelty, disruptive potential, and rapid advancement.
   - **c.** Augmented reality, virtual reality, Internet of Things and artificial intelligence can be considered emerging technologies.
   - **d.** The progressive nature of these technologies allows for synergies with other technologies.

2. What term refers to digital money used for online transactions?
   - **a.** artificial intelligence
   - **b.** blockchain
   - **c.** bitcoin
   - **d.** augmented reality

3. Which statement best describes the convergence of frontiers of information systems and emerging technologies?
   - **a.** Connecting Internet of Things and devices creates a disruptive environment and negatively impacts user experiences.

b. It enables organizations to create new opportunities for innovation and growth.
c. Blockchain combined with augmented reality and virtual reality can lead to profit losses for organizations.
d. The role of data analysts will no longer be needed as the convergence of emerging technologies and innovation systems has the potential to accomplish analysis-related tasks.

4. Frontiers of information systems present several opportunities, challenges, and risks for use. Which of the following is an opportunity?
   a. It can increase compatibility between networked systems.
   b. It will lead to a reduction in hardware and software costs, increasing the overall costs of processing data.
   c. Data breaches become of increasing concern.
   d. Adherence challenges to regulatory compliance requirements may be at risk.

5. Which of the following is true about societal and global impacts of emerging technologies?
   a. They only affect small groups.
   b. Emerging technologies have only had a small effect on communities.
   c. Academia is the only area of societal change.
   d. Artificial intelligence–enabled systems are examples of the societal and global impacts of emerging technologies.

6. Why is solar power considered an emerging technology?
   a. It has seen widespread adoption, helping consumers to lower their electricity bills.
   b. Laws have been passed to prevent companies from marketing these products to consumers.
   c. Economies have been negatively impacted by its widespread use.
   d. It has decreased dependency on fossil fuels.

7. How do data analytics support health-care efforts?
   a. It helps to identify different strands of the flu and its prevalence in communities.
   b. The data collected reduce efficiencies in health care–related supply chains and logistics.
   c. It provides information on health-care resourcing to help organizations identify staffing and financial needs.
   d. It helps to initiate targeted marketing campaigns aimed at increasing awareness and disease prevention.

8. Which is not a correct statement about research and innovation in technology?
   a. It has contributed to significant growth in the data analytics and predictive analytics markets.
   b. Global growth in technologies has been experienced in several countries in varying sectors of business.
   c. Research and innovation activities further new findings, technologies, and processes.
   d. It has been funded primarily by governments in all countries.

9. What is the purpose of research as it relates to technology?
   a. It is the precursor to innovation.
   b. It is a secondary component within the design process.
   c. Research provides the full picture of how the technology is supposed to function.
   d. Research prevents innovation from being adopted by consumers.

10. Which of the following is a true statement about the process of innovation?
    a. It follows the systematic steps: conception, implementation, marketing, and communication.
    b. Analyzing and recording information is the first step in identifying and selecting resources.
    c. The scientific research process and associated skills are at the core of the research process.
    d. Information must be recorded and communicated immediately.

11. Which of the following is a false statement as it relates to the Internet of Things in health care?

a. It enhances patient monitoring capabilities, medication adherence, and overall well-being.
b. It supports the distribution of medical information.
c. Patients can use their mobile devices to check the results of medical tests.
d. It creates challenges in videoconferencing with the medical care team.

Check Your Understanding Questions

1. What are the major differences between virtual reality and augmented reality?
2. What is the U.S. Department of Energy's relationship to emerging technologies?
3. Describe how blockchain technology supports the safe use of cryptocurrency.
4. How do augmented reality and virtual reality enhance user shopping experiences?
5. What is the difference between emerging technologies and frontiers of information systems?
6. What are the main goals in using different tools and techniques in data analytics?
7. What are some opportunities provided by mobile computing technologies?
8. What is a drawback to not analyzing big data in a timely manner?
9. What is the relationship of emerging technologies and society from a global perspective?
10. How are businesses able to leverage e-commerce functions using social media?
11. How does data analytics support education?
12. What is the importance of research in innovation?
13. How do research and innovation lead to emerging technologies?
14. What is the purpose of fostering collaboration of stakeholders in creating ethical and responsible use of emerging technologies?
15. How does the identification of emerging trends in cybersecurity help to create a cyber-resilient information system?

Application Questions

1. Discuss the benefits of blockchain technology in health-care organizations.
2. Watch this Wall Street Journal video (https://openstax.org/r/109BatteryPlant) that highlights an engine factory in Germany that is being transformed into a battery plant. Why is so much software development involved in the making of electric vehicles? Why might electric vehicle start-ups have a certain advantage in writing software? Why might software development be a difficult task for traditional automakers like VW to manage?
3. Discuss how banks have optimized many of their customer service functions with the use of artificial intelligence.
4. Describe how frontiers of information systems technology is used to enact positive social change.
5. Business process outsourcing has evolved as a major technology-supporting industry. Discuss the importance of business process outsourcing and its impact on the industry.
6. How has the evolution of technology changed telemedicine?

11

Global Information Systems

Figure 11.1 By utilizing digital innovation to become a smart city, Dubai, in the United Arab Emirates, has been improving public safety, energy efficiency, sustainability, and overall quality of life. (credit: modification of work "High High ... High Enough to Dream" by Maher Najm/Flickr, Public Domain)

Chapter Outline

Introduction

With digital innovation and advancements in global information systems, the world has become more tech savvy and interconnected. An example is the rise of smart cities, such as Dubai in the United Arab Emirates. In partnership with government agencies and private-sector organizations, the Digital Dubai Office has over 130 initiatives intended to digitalize daily life in Dubai, making the city a better place to live as it becomes more efficient and competitive in the world marketplace. This even includes an initiative to make Dubai the happiest city on earth.[1] Through this initiative, the city discovers what Dubai citizens need and want to be happy and then uses technology to meet those needs. As a result, there have been robust changes in the city's housing, transportation system, and health-care services to promote Dubai citizens' well-being.

11.1 The Importance of Global Information Systems

Learning Objectives

By the end of this section, you will be able to:

- Explain the fundamentals and importance of global information systems
- Distinguish between global information systems and traditional information systems
- Describe the infrastructure of global information systems

The business world is a network of interconnected companies operating across various continents linked by technology. This technology supports communication and collaboration with other businesses and

1 "Happiness Agenda," Digital Dubai, accessed January 26, 2025, https://www.digitaldubai.ae/initiatives/happiness-agenda

geographically dispersed teams. The smooth interchange of information is critical to global business operations. How is this accomplished? At the center of global information interchange lies a complex system known as a **global information system**, an intricate network of hardware, software, data, and telecommunications infrastructure that enables information collection, storage, management, processing, analysis, and dissemination worldwide. Global information systems are the backbone of international operations, allowing organizations to exchange information, communicate effectively, and collaborate. Global information systems enable companies to overcome geographical barriers and tap into new opportunities for growth and innovation through knowledge sharing.

As Figure 11.2 shows, a global information system manages and analyzes information across countries and regions to support worldwide operations and decision-making. You can think of a global information system as an information hub—similar to a library—collecting, storing, managing, processing, analyzing, and disseminating information. The global information system is continually updated, providing real-time insights across geographic boundaries.

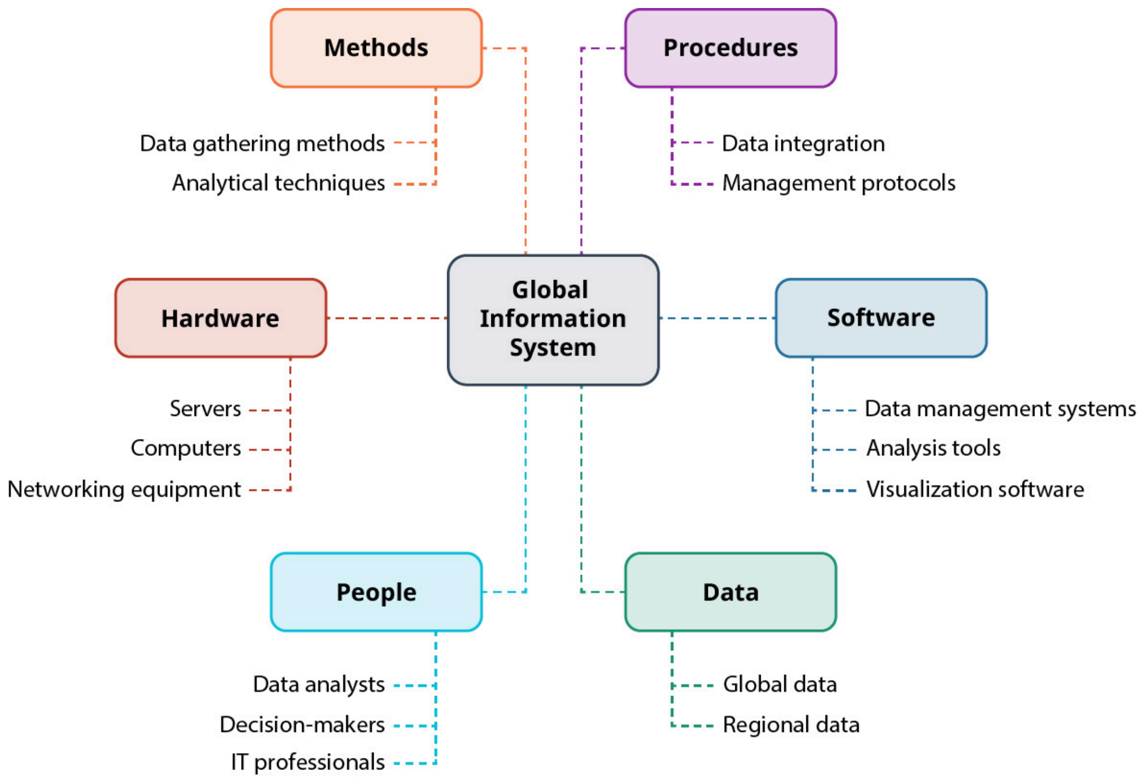


Figure 11.2 The elements that make up a global information system are the methods, procedures, hardware, software, people, and data to process and share global data effectively, which differentiate these systems from more local information systems. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

A good example of a global information system is Tesla's use of over-the-air (OTA) software updates. This system lets Tesla update its cars remotely, thereby improving performance, adding new features, and fixing problems without customers needing to go to a service center. The strategic impact of OTA updates is significant: they keep Tesla's cars technologically advanced and continuously improve the customer experience, providing a key competitive advantage in the automotive industry. This system reduces costs associated with physical recalls and enhances the long-term value of Tesla vehicles, demonstrating how a global information system can facilitate cross-border collaboration and support sustainable growth in a complex global marketplace.[2]

2 Katie Rees, "What Are Tesla's Over-the-Air Updates?," MakeUseOf, October 21, 2023, https://www.makeuseof.com/what-are-tesla-over-the-air-updates/

You may come across a similar term, "geographic information system," often abbreviated as "GIS," but this type of system focuses on managing spatial or geographic data, including maps, satellite imagery, and location-based information. Geographic information systems can analyze terrain data for urban planning or track wildlife migration patterns, or support emergency response efforts. For example, during Hurricane Helene in 2024, emergency teams used geographic information systems to analyze flood risk zones, prioritize evacuations, and identify isolated communities.[3] This real-time data helped responders prioritize evacuation orders and deploy rescue resources. There are many important applications of geographic information systems as a system themselves or as part of a global information system. A geographic information system can be a component of a global information system, but the latter may also include enterprise resource planning systems, global supply chain management systems, and customer relationship management systems that manage global operations. Many examples related to geographic information systems reinforce concepts that involve solving local problems, but the solutions can be applied to larger, more complex problems around the world.

Global information systems play a different role. While global information systems may still include geographic data, the main goal is to help individuals, organizations, and governments connect and collaborate across the globe. An example of a global information system that many of us experience is Google Ads. When you search for a product, such as running shoes, on Google, you might notice ads for different brands appearing at the top of the search results. These ads are targeted specifically to you using data from your search history, location, and online behavior, whether you're in New York, Tokyo, or Paris. Google Ads allows businesses to reach potential customers like you across the globe with personalized marketing, increasing the chances that their ads are relevant, driving sales, and maximizing their return on investment.

The Role of Global Information Systems

Global information systems are essential components of modern society and play a critical role by enabling organizations to coordinate operational activities on a global scale. For instance, Netflix uses a global information system that leverages big data and machine learning algorithms to recommend movies and shows to users across different countries, based on their viewing history, preferences, and behaviors.[4]

One use of global information systems is to track the movement of raw materials across various continents, predict the path of a hurricane, or help you find the nearest shipping center. These systems are woven into society, shaping everything from global business efficiency to disaster response effectiveness. They also accelerate international expansion by providing organizations with the necessary infrastructure to enter new markets, adapt to diverse regulatory environments, and compete globally. For multinational corporations, global information systems streamline processes such as supply chain management, allowing for seamless coordination of production, distribution, and logistics operations across borders. In addition, global information systems support the standardization of business practices and workflows, ensuring consistency and efficiency across global operations. Global information systems are useful for breaking geographic barriers, facilitating global connectivity, and fostering global citizenship.

Global information systems can also allow companies to overcome geographical barriers by providing a platform for sharing knowledge and resources regardless of physical distance. This opens new opportunities by tapping into global talent—skilled professionals from around the world—which allows for collaboration, leveraging diverse skills, and exploring new markets.

A global information system enables individuals, organizations, and governments to connect and collaborate across vast distances. Through email, videoconferencing, social media, and other digital platforms, global information systems have transformed how people communicate and share information, transcending local barriers of time and location. For example, a medical team in Montreal can consult with a specialist about a

3 "Navigating Devastation: GIS Aids Hurricane Helene Response," Esri ArcNews, Winter 2025, https://www.esri.com/about/newsroom/arcnews/navigating-devastation-gis-aids-hurricane-helene-response/
4 Miriam Chandi, "How Does Netflix Use Technology to Improve Their Business?," Start Motion Media, September 23, 2024, https://www.startmotionmedia.com/how-does-netflix-use-technology-to-improve-their-business/

patient located in a remote Nordic village using videoconferencing software.

Another benefit of a global information system is that it can promote global citizenship by increasing awareness of international issues and facilitating cross-cultural understanding. This is accomplished by providing access to information, educational resources, digital tools, online forums, or interactive platforms where individuals, organizations, and communities can actively engage in decision-making processes, share knowledge, collaborate on projects, and contribute to discussions.

In addition to international connections, global information systems can grow businesses by nurturing innovation and creativity, enhancing operational efficiency, and supporting informed decision making. Global information systems encourage innovation and creativity within organizations. Global teams can collaborate on projects, share ideas, and leverage diverse perspectives as they develop innovative solutions to complex problems. For example, cross-continental meetings where teams work together in real time to tackle specific challenges and prototype new ideas allow employees the opportunity to contribute ideas and refine concepts collaboratively.

Global information systems can also support informed decision-making: In crises like natural disasters or epidemics decision-makers need accurate, timely data to respond effectively. A global information system integrates and visualizes data from sources like weather patterns, population density, and resource availability. By providing clear, actionable insights, global information systems help decision-makers improve business operations, policy development, and strategic planning.

Finally, global information systems streamline business processes, improve workflow efficiency, and optimize resource allocation. Logistics companies—like FedEx, UPS, and DHL—can optimize delivery routes based on traffic conditions displayed through systems, saving time and fuel, leading to cost savings and improved customer service (Figure 11.3). Utility companies can pinpoint the source of outages by analyzing real-time data on power grids and infrastructure, leading to faster repairs and improved service.

Figure 11.3 A global information system allows a delivery business, like FedEx, to optimize its delivery routes and meet its customers' needs. (credit: modification of work "MEM FedeEX flight line" by Steve Knight/Flickr, CC BY 2.0)

Let's look at global information systems in action by looking at Nike. Nike uses global information systems to manage its extensive global supply chain, which spans from factories in Vietnam to stores worldwide. Global information systems enable Nike to track raw materials, streamline production, and optimize delivery routes, ensuring timely and cost-effective operations. Beyond logistics, global information systems help Nike identify new market opportunities, such as expanding into South America, by analyzing data to tailor marketing strategies and product offerings. Global information systems help Nike manage inventory and track customer preferences across various regions. This integration supports Nike's e-commerce platform by providing accurate inventory levels and efficient order fulfillment globally. Additionally, global information system data allow Nike to tailor online marketing strategies and product recommendations based on regional trends and consumer behavior, ensuring a personalized shopping experience and effective market expansion.[5]

Another example is the Real-Time Air Quality Index Visual Map that provides real-time information about the air quality and air pollution in different regions of the world.[6] The map helps those traveling to make informed decisions concerning their destinations, especially if they have any form of respiratory disease.

ETHICS IN IS

Global Information Systems for Humanitarian Efforts

The United Nations (UN) uses global information systems to boost its humanitarian efforts around the world. One notable example is during the Syrian refugee crisis.[7] As millions of Syrians fled their homes to escape conflict, the UN relied on geographic information systems to coordinate aid distribution, track refugee movements, and plan the establishment of refugee camps. These allowed UN agencies and humanitarian organizations to analyze satellite imagery to identify suitable locations for refugee camps, considering factors such as accessibility, terrain, and proximity to essential services like water sources and medical facilities. Working in conjunction, global information systems helped with the integration of various datasets, encompassing not only geographic data but also nonspatial information from diverse sources, such as demographic data, epidemiological data, health-care infrastructure, and disease transmission patterns from multiple regions worldwide. This data-driven approach helped foster international collaboration and cross-border coordination between UN agencies and other humanitarian organizations to optimize the placement of camps to ensure efficient delivery of aid and support to displaced populations.

How Global Information Systems Differ from Traditional Information Systems

Consider a logistics company with warehouses scattered across the globe. A traditional information system might track inventory levels within each warehouse but wouldn't be able to show the bigger picture—the real-time location of shipments, customer preferences based on location, or potential bottlenecks in the supply chain. This is where a global information system comes into play.

Global information systems are designed to manage and handle the complexities of global operations. Unlike traditional information systems, which are typically limited to a specific geographic location or organizational boundary, global information systems excel at handling and managing data regardless of geographic location. Characteristics that set a global information system apart from a traditional information system (Figure 11.4) include its global reach, the types of data it works with, and its integration with other systems.

5 CleanChain Editorial Team, "How Does Nike's Supply Chain Work?," ADEC Innovations, May 12, 2020, https://www.adec-innovations.com/blogs/how-does-nikes-supply-chain-work/
6 "Air Pollution in World: Real-Time Air Quality Index Visual Map," The World Air Quality Index Project, accessed January 26, 2025, https://aqicn.org/map/world/
7 Eyad Ghattasheh, "Managing Syrian Refugee Camps Using ArcGIS," Esri ArcUser, Fall 2017, https://www.esri.com/about/newsroom/arcuser/managing-syrian-refugee-camps-using-arcgis

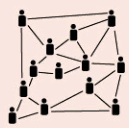
	Global Information Systems	Information Systems
Scope of operations 	Designed to facilitate communication, collaboration, and decision-making across multiple organizations and geographic boundaries; equipped with advanced features such as multilingual support, currency conversion, and internationalization capabilities	Focuses on supporting the internal operations of a single organization or a specific geographic region
Data structure 	Deals with unstructured or semi-structured data; requires more sophisticated processing techniques, such as data mining, natural language processing, and machine learning	Typically deals with structured data, such as sales transactions or inventory levels
Integration 	Characterized by its ability to integrate and analyze data from multiple sources including internal systems, external databases, and the internet	Focuses on a more localized system integration

Figure 11.4 A GIS and an IS differ in their location reach, data structure, and integration capabilities. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

One of the key differences between a global information system and a traditional information system is their scope of operations. While a traditional information system is focused on supporting the internal operations of a single organization or a specific geographic region, a global information system is designed to facilitate communication, collaboration, and decision-making across multiple organizations and geographic boundaries. This allows users to see the entire operation across the globe, from bustling city centers to remote rural areas. In addition, a global information system is equipped with advanced features such as multilingual support, currency conversion, and internationalization capabilities to accommodate the diverse needs of organizations worldwide. A traditional information system is typically designed for internal data management within a single organization or a specific geographic region. An information system might track sales figures for all of a company's stores, but it wouldn't inherently know each store's physical location or how sales figures relate to other factors like demographics or traffic patterns.

While both traditional information systems and global information systems manage data, they handle them in a fundamentally different way. A traditional information system typically deals with structured data, such as sales transactions or inventory levels, which are relatively straightforward to manage; they are organized and categorized in a predefined format. Imagine a customer database that includes columns for a customer's name, address, phone number, and purchase history. Each piece of data occupies a specific slot, making it easy for the information system to store, retrieve, and analyze. However, a traditional information system struggles with the complexity of geographic data that come in a variety of formats. A global information system often deals with unstructured data, which do not have a predefined organization, or semi-structured data, which are somewhat organized but lack the fixed schema of a traditional database. Examples of unstructured and semi-structured data include social media feeds, sensor data (information collected by a device that detects and responds to a physical input, such as temperature), and satellite imagery. These types of data require more sophisticated processing techniques, such as data mining, natural language processing, and machine learning, to extract meaningful insights. Consider a utility company managing a network of power lines. A traditional information system might struggle to analyze outages based on location. However, since a global information system has the ability to model the network's spatial layout, the company can pinpoint the outage zones and identify affected customers much faster. This specialized data structure empowers a global information system to unlock the full potential of location-based data for analysis and visualization.

Finally, a global information system is characterized by its ability to integrate and analyze data from multiple sources, including internal systems, external databases, and the internet, enabling a more complete picture to emerge. Sales trends can be analyzed alongside weather patterns, or delivery routes can be optimized based on traffic congestion in a specific area. This integration capability is essential for supporting global operations as it allows organizations to access and combine data from different sources to gain a comprehensive view of their operations and make informed decisions.

Facilitating Communication and Collaboration with Global Information Systems

A global information system facilitates communication and collaboration across different locations by transcending the barriers of distance, time zones, cultural differences, and language barriers. This transformative power of global information system empowers organizations to operate seamlessly on a global scale, a feat that was once considered nearly impossible.

Integration of Operations

A global information system enables organizations to integrate their operations across locations, facilitating centralized data management, streamlined processes, and operational consistency. For instance, a multinational corporation like Toyota leverages global information systems to integrate its manufacturing, distribution, and sales operations across the globe.[8] This integration is essential for achieving economies of scale, reducing duplication of efforts, and optimizing **resource utilization**, which is the efficient and effective allocation and management of resources such as time, money, materials, or personnel to achieve desired objectives or outcomes. By harnessing global information system capabilities, Toyota is consistent in product quality and operational efficiency across its worldwide operations. This is imperative for business competitiveness and customer satisfaction, as well as for driving innovation and organizational agility.

Real-Time Communication

A global information system provides real-time communication tools such as email, instant messaging, and videoconferencing, allowing employees in different locations to collaborate and communicate effectively. Consider SpaceX's international project team. Team members must communicate effectively, address technical challenges promptly, and ensure project milestones are met on time.[9] Global information system-enabled videoconferencing and instant messaging tools allow real-time communication for coordinating activities and resolving issues quickly, enhancing project success. An added benefit is that this technology can help foster a sense of teamwork among geographically dispersed teams despite being separated by thousands of miles.

Access to Global Information

A global information system provides a wealth of global information including market trends, competitor analysis, regulatory requirements, and cultural insights. This information is essential for making informed decisions, identifying new opportunities, and mitigating risks associated with global operations.

Standardization of Processes

A global information system enables organizations to standardize processes and procedures across different locations, ensuring consistency in quality, compliance, and performance. This standardization is essential for maintaining brand reputation, meeting customer expectations, and achieving operational excellence. For instance, multinational banks leverage global information systems to standardize compliance procedures across branches worldwide, ensuring regulatory compliance and reducing operational risks.

8 Hassan Ali, "Toyota's JIT and AI: A Powerful Combination for Supply Chain Optimization," LinkedIn, October 3, 2024, https://www.linkedin.com/pulse/toyotas-jit-ai-powerful-combination-supply-chain-optimization-ali-knoie/
9 Maria Thomas, "How SpaceX is Transforming Project Management Practices," MPUG, https://mpug.com/how-spacex-transforming-project-management-practices/

Cost Reduction and Customer Satisfaction

A global information system can help reduce costs associated with global operations by enabling organizations to optimize their supply chain, reduce inventory levels, and minimize travel expenses. FedEx, for example, uses a global information system to reduce operating costs and enhance profitability while maintaining service quality. By analyzing transportation routes and warehouse locations, minimizing shipping distances, consolidating inventory, and optimizing resource allocation, FedEx can deliver expediently to its customers, and this customer-centric approach is essential for building loyalty and driving repeat business.[10]

While a global information system can lead to cost reductions for organizations with global operations, it is important to recognize that there may be higher costs initially due to the complexity of the system's size and its scope of connectedness. While global information systems offer cost-saving opportunities in future years, organizations must carefully manage these complexities to ensure overall financial sustainability.

Improving Decision-Making Processes with Global Information Systems

Whether strategic, operational, or tactical, decisions influence every aspect of an organization's performance, from resource allocation to market positioning. In today's dynamic and competitive business environment, the ability to make timely and informed decisions is essential for organizations to thrive and adapt to change. A global information system facilitates comprehensive analysis, providing decision-makers with a holistic view of the factors influencing their operations. For example, a retail chain may use a global information system to integrate sales data with demographic information, helping them make informed decisions about where to expand and how to increase their presence in the global market.

Visualization of Spatial Data

Visual representation is a powerful tool for understanding complex data and communicating insights effectively (see 8.2 Foundations of Business Intelligence and Analytics). Within a global information system, a geographic information system enables organizations to visualize spatial data through interactive maps, charts, and dashboards. The term **spatial analysis** refers to the process of examining patterns, trends, and relationships within geographic data to gain insights and make informed decisions about spatial phenomena. By using spatial analysis, decision-makers gain valuable insights, visualize complex information, and develop informed strategies. Imagine you have a map of your neighborhood with all the places where people have complained about noisy pet dogs. Spatial analysis would help you see if the complaints are clustered in certain areas or spread out. This way, you could find out if there's a pattern, like if noisy dogs are more common near certain types of homes or parks, helping you decide where to focus your efforts to address the issue. Another example would be a city planning department using geographic information system maps to visualize population density, land-use patterns, and transportation networks to inform urban development strategies.

Scenario Models and Predictive Analysis

Anticipating future trends and outcomes is essential for proactive decision-making. A geographic information system allows organizations to assess the potential impacts of various strategies and courses of action by conducting **predictive analysis**, which is the use of data, specifically statistical algorithms, to help organizations identify patterns and make predictions that will enhance the operational results (see more about predictive analytics in 8.2 Foundations of Business Intelligence and Analytics). By simulating various scenarios and analyzing their potential outcomes, decision-makers can evaluate risks, identify opportunities, and develop robust strategies to achieve their goals. Utility companies leverage GIS-based predictive analysis to forecast electricity demand and optimize infrastructure investments, ensuring efficient resource allocation and strategic planning.

10 Jacquelyn Haas, Jeff McLeod, Rick Dezemplen, and Rodney Conger, "Using GIS in Strategic Planning and Execution at FedEx Express" (paper presented at ESRI 2010 International User Conference, Paper: 1520), https://proceedings.esri.com/library/userconf/proc10/uc/papers/pap_1520.pdf

Geographic Context and Spatial Relationships

Understanding **geographic context**, or considering the impact of location on operations, is critical for making informed decisions, especially in urban planning, natural resource management, and emergency response. For instance, a forestry company may use a geographic information system to assess the location and distribution of timber resources, environmental constraints, and market demand. By incorporating geographic context into decision-making processes, organizations can mitigate risks, optimize resource allocation, and maximize opportunities for success.

FUTURE TECHNOLOGY

Geographic Information Systems for Emergency Response Planning

The city of Los Angeles stands out for its innovative use of geographic information system technology in bolstering its emergency response planning processes, leveraging its functionalities at each stage with precision.[11] The city not only optimizes local emergency response efforts but connects to global resources, such as best practices and disaster models. For instance, lessons from other earthquake-prone cities like Tokyo inform how Los Angeles prepares its evacuation routes and resource allocations.

A geographic information system integrates a plethora of datasets from various sources, encompassing population demographics, infrastructure locations, and emergency response resources into a centralized platform. This consolidation provides decision-makers with a holistic view of the city's physical features (like roads, buildings, hospitals, and fire stations) as well as demographic data (population density, vulnerable communities) and infrastructure elements (utilities, communication network)—in other words, the city's landscape—facilitating cross-disciplinary analysis and informed resource allocation to identify and address gaps in emergency response readiness.

By visualizing critical infrastructure data such as hospitals, fire stations, and evacuation routes, alongside demographic data, city officials communicate emergency plans to the public and coordinate response efforts across various agencies. A geographic information system enables detailed scenario planning by simulating complex disaster scenarios such as earthquakes and wildfires across the city's vast and varied terrain. Decision-makers evaluate the potential impacts of each scenario, leveraging spatial data to assess resource requirements and communicate collaboratively. Notably, the city makes much of its mapping data available to residents of the LA area, and facilitates neighborhood use of its geographic data.

The result is comprehensive contingency plans that are tailored to mitigate risks and ensure a coordinated response. Through geographic information system platforms, stakeholders from different departments and agencies throughout the city can share information, exchange insights, and coordinate efforts. A geographic information system enables communication with international agencies when necessary, extending its reach into a global information system and allowing for the integration of global best practices and resources into local emergency response strategies.

Global Information System Infrastructure

A **global information system infrastructure** refers to the foundational framework of hardware, software, data storage, network, and cloud-based services that support global information system operations within an organization. It serves as the backbone for managing, analyzing, and visualizing spatial data to support decision-making, operational efficiency, and strategic planning on a global scale. This intricate network, much like the nervous system of a living organism, serves as the conduit for the flow of information that empowers global communication, economic exchange, and organizational advancement. A robust global information

11 Ron Galperin, "Get Ready, Stay Prepared: A Guide to Emergency Planning in the City of Los Angeles," L.A. Controller Ron Galperin, accessed January 7, 2025, https://storymaps.arcgis.com/stories/d32f5d0d03d64964be022b0de6c2b290

system infrastructure ensures reliability, scalability, and performance, allowing organizations to derive maximum value from collective information.

The global information system infrastructure is built on the interconnection of local, national, and international communication networks. This includes infrastructure like fiber optic cables, satellites, and communication towers that transmit data and connect hardware devices, software applications, and data storage systems across the globe. Reliable network infrastructure supports data sharing, communication, and collaboration within global information system environments. The network infrastructure encompasses network components such as routers, switches, firewalls, and wireless access points that facilitate data exchange and collaboration. Common network architectures include client-server, peer-to-peer, and cloud-based architectures.

Cloud computing services are accessible anywhere in the world with an internet connection, empowering employees, partners, and clients to connect and collaborate in real time. Cloud providers work hard to ensure availability of their services, meaning they are operational nearly 24/7, further enhancing communication reliability. Storage area networks are high-speed networks specifically designed to connect storage devices to servers. They allow for faster data access compared to traditional storage solutions.

Communication protocols are an established sets of rules that govern how devices communicate within the global information system infrastructure. They define how data are formatted, transmitted, and received, ensuring compatibility between different systems and software applications. Common protocols include TCP/IP (Transmission Control Protocol/Internet Protocol) and HTTP (hypertext transfer protocol) and FTP (File Transfer Protocol).

An **interoperability standard** is a guideline, protocol, or specification that enables different systems, technologies, or platforms to communicate, exchange data, or work together seamlessly. Security measures, such as encryption and access controls, safeguard global information system infrastructure from unauthorized access and breaches. Scalability and flexibility allow the systems to adapt to evolving needs and technological advancements, while maintenance and support ensure optimal performance through updates and troubleshooting.

ETHICS IN IS

Beyond the Essentials: Security and Safeguarding Data

Ethics in a global information system focuses on security and privacy. Interoperability standards ensure that different systems can work together effectively, protecting user privacy and maintaining trust. These standards provide a common framework for system compatibility and data exchange. Security measures, such as encryption and access controls, are vital for preventing unauthorized access and protecting data integrity. Together, these practices ensure that data are handled responsibly and ethically. Public health agencies often rely on global information system infrastructure to help track and analyze the spread of infectious diseases. Patient locations and demographics of reported cases allow for targeted interventions and resource allocation.

Security measures like encryption and access controls are critical to protect data and ensure public trust. Encryption scrambles data into an unreadable format, making it virtually impossible for unauthorized users to access confidential information even if intercepted. Access controls determine who can view, edit, or delete specific data within the system's infrastructure. These controls can be implemented through user authentication and role-based access permissions. It's important to note that different organizations maintain their own datasets, and protocols must account for this diversity in data management and security.

Hardware

The global information system infrastructure also relies on a variety of hardware and software components to function. Hardware includes computers, workstations, routers, and peripherals, such as cables, printers, and scanners, and encompasses servers, storage devices, and end-user devices necessary for processing and storing data. High-performance servers for data processing and storage are essential for handling the large volumes of data exchanged in global operations. These devices handle the computational demands of operations, enabling faster data processing, storage, and retrieval and enhancing the overall efficiency and performance of workflows. Compared to traditional IT hardware, global information systems need more specialized equipment. While standard servers and workstations are fine for general business tasks, global information system hardware is designed for high-performance computing and large data storage. For example, global information systems often uses fiber optic cables, which offer faster data transfer and less interference than traditional copper cables.

Software

Software components include operating systems, communication protocols, and applications and tools needed to create, edit, analyze, and share data effectively. A global database is akin to a vast library containing information from around the globe. For example, a global database might keep track of environmental data, like deforestation and pollution, which people across the world can use to make decisions. It serves as a central repository that can be accessed and analyzed on a global scale. Robust data storage solutions enable organizations to store and retrieve data efficiently, supporting real-time analysis, decision-making, and collaboration.

Global information system-specific applications—such as those for supply chain management and customer relationship management—allow organizations to navigate complexities, optimize processes, and deliver exceptional value across their supply chains, customer relationships, and strategic decision-making endeavors. A company’s supply chain management (SCM) software helps them manage goods and services from the point of origin to the point of consumption. It includes tools for planning, sourcing, production, inventory management, and logistics. This software provides real-time visibility into the supply chain, enabling organizations strategize effectively. For example, Starbucks uses a global information system to optimize its global coffee supply chain. By mapping coffee farms, tracking product quality, and assessing climate change risks, Starbucks ensures a reliable and sustainable supply of coffee beans. This technology helps the company improve efficiency, reduce costs, and support sustainable practices.[12]

A customer relationship management (CRM) software system encompasses the management of customer interactions throughout their life cycle, aiming to enhance satisfaction and foster loyalty. A CRM merges data from disparate sources like sales, marketing, and customer service into a centralized database. This integration empowers organizations to delve into customer behavior, tailor marketing initiatives, and refine service delivery. The benefits include heightened customer satisfaction and loyalty, increased retention rates, expanded cross-selling and upselling prospects, and enriched insights facilitating informed decision-making.

Designing and Implementing a Global Information System Infrastructure

Building a robust global information system infrastructure requires thorough planning and execution to align with an organization’s strategic goals and operational needs. Figure 11.5 shows the steps for designing and implementing a global GIS infrastructure.

12 "Starbucks Supply Chain Management: Optimizing Global Coffee Distribution Through Risk Mitigation and Sustainable Practices," SFK Inc., SKK Marine, SFK SecCon, July 19, 2024, https://sfkcorp.com/starbucks-supply-chain-management-optimizing-global-coffee-distribution-through-risk-mitigation-and-sustainable-practices/

Global Information System Infrastructure	
STEP 1	Understanding the organization's needs
STEP 2	Defining clear objectives
STEP 3	Assessing technology needs
STEP 4	Selecting the right technologies
STEP 5	Designing the infrastructure
STEP 6	Phasing implementation
STEP 7	Training and ongoing support
STEP 8	Continuous monitoring and maintenance
STEP 9	Soliciting feedback and improvement

Figure 11.5 Most companies follow these nine basic steps when designing a global information system infrastructure. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Step 1: Understanding the Organization's Needs

Start by conducting a thorough assessment of the organization's specific requirements, considering factors such as size, geographic distribution, operational scope, and information needs. Decision-makers at Toyota, for example, would consider the company's manufacturing, distribution, and sales operations across continents, with the goal of improving economies of scale and operational efficiency.

Step 2: Defining Clear Objectives

Establish SMART (specific, measurable, achievable, relevant, and time-bound) objectives for the global information system infrastructure that contribute to the organization's business goals. For instance, SpaceX could aim to increase collaboration efficiency among international project teams by 30 percent within six months, with an anticipated result of a 15 percent reduction in spacecraft development time by the end of the fiscal year.

Step 3: Assessing Technology Needs

Conduct a comprehensive needs assessment of technology requirements A needs assessment is the gathering and analyzing of data to identify and evaluate the current state, areas for improvement, and interventions needed to get to a more improved state It should include the following:

- hardware and software needs
- network infrastructure and security considerations
- scalability and interoperability with existing systems
- ability to handle future growth in data volume and users

For example, in a needs assessment, consumer goods company Procter & Gamble would consider the technology requirements for accessing market trends and competitor analysis data in new markets. They would evaluate the necessary hardware and software to support data analysis, ensure their network infrastructure can securely handle the influx of data and users, and verify that their systems can scale and integrate with existing platforms. This needs assessment will help to tailor marketing strategies and optimize product portfolios.

Step 4: Selecting the Right Technologies

Based on the needs assessment, choose the most suitable technologies with cost, reliability, performance, and vendor support in mind. Explore options like cloud services, enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, and other relevant applications, such as business intelligence (BI) tools. For example, FedEx considered the cost, reliability, performance, and vendor support needed to optimize transportation routes and strategically locate warehouses, minimizing shipping distances and enhancing customer satisfaction.

Step 5: Designing the Infrastructure

In designing the infrastructure, carefully consider the following:

- network setup
- data storage and management strategies
- robust security measures
- comprehensive disaster recovery plan
- scalability, flexibility, and the ability of the design to support future growth

The planning team for the city of Los Angeles would consider this list in designing a global information system infrastructure that will use a geographic information system to visualize population density, land-use patterns, and transportation networks in order to inform urban development strategies.

Step 6: Phasing Implementation

The infrastructure should be implemented in phases. Start with a pilot project to test the infrastructure and use what is learned during the pilot to refine the system before a full rollout. Adding this step helps to correct any issues and fix any bugs in the system before full deployment. Make sure to develop clear documentation and communication plans and keep stakeholders informed. For example, the Federal Emergency Management Agency launched a pilot program as part of its implementation for decision-making and response during emergencies before rolling out the full program. The pilot program revealed ways to improve hazard mitigation plans, such as methods to use artificial intelligence and provide communities with customized disaster preparedness and response plans that meet citizens' specific needs in a geographic area.

Step 7: Training and Ongoing Support

To ensure proficient use of the global infrastructure, it is necessary to train employees. This includes developing and implementing user manuals and help desks to address initial challenges. For example, Target has trained its employees to use a global information system to track customers' locations in real time. With this information, employees bring orders to the front of a store just in time to place the order in a customer's automobile as soon as they arrive at the store. Not only does this minimize the amount of time that customers must wait, it also ensures that perishables, such as frozen goods, do not spoil while customers are en route to pick up their orders.

Step 8: Continuous Monitoring and Maintenance

It is imperative to implement a regular monitoring plan to ensure optimal infrastructure performance. Schedule routine maintenance to keep the system up to date with the latest security patches and ensure smooth operation. Make sure any issues are promptly addressed to minimize downtime.

Step 9: Soliciting Feedback and Improvement

Actively solicit and implement user feedback to drive continuous improvement. This ensures the system's infrastructure evolves to meet the organization's ever-changing needs, optimizing service quality and efficiency.

Challenges of Managing a Global Information System Infrastructure

Managing a global information system infrastructure demands skilled navigation of various challenges, such as data interoperability and accuracy, security and privacy concerns, legal and regulatory compliance, infrastructure resilience, and disaster recovery mechanisms.

Data Interoperability and Accuracy

Ensuring data interoperability, accuracy, and compatibility across diverse systems and sources is a major challenge. The ability of diverse data systems or formats to exchange, integrate, and interpret data accurately and efficiently is considered **data interoperability**, and it often includes processes like data cleaning and standardization (see Chapter 2 Data Management and Information Systems Business Strategies). The accuracy of data is vital, and organizations may use a variety of software and data formats, making exchanging and integrating data difficult. Managing the system's infrastructure across regions requires hardware and software platform compatibility. Optimization of the performance of global information system infrastructure is needed to ensure that it meets the needs of users and applications. This includes monitoring performance metrics, identifying bottlenecks, and implementing measures to improve performance, such as hardware upgrades or software optimizations.

Security and Privacy

From customer demographics to classified project locations, an organization's global information system holds a wealth of sensitive information that needs protection. It is imperative to protect sensitive data from unauthorized access and breaches and ensure compliance with data sovereignty laws and intellectual property rights. Security tools such as encryption, firewalls, intrusion detection systems, and multi factor authentication are crucial in protecting this data.

Infrastructure Resilience

To ensure a global information system's infrastructure remains resilient in facing a cyberattack, organizations must proactively prepare for the worst-case scenario and build systems that can weather the attack. By implementing robust cybersecurity measures and fortifying the physical infrastructure, such as servers, data centers, and networking equipment, from risks (such as natural disasters, power outages, theft), organizations can minimize downtime, protect data, and keep operations running smoothly.

Cost and Scalability

A global information system infrastructure is complex, involving a wide range of hardware, software, data, and networks that must work together seamlessly. Managing this complexity requires careful planning, coordination, and technical expertise to ensure all components are integrated and functioning properly. Other challenges with global information system infrastructure include cost and scalability. A global information system infrastructure involves investments in hardware, software, data, and networks, as well as ongoing maintenance and support costs. Balancing these costs with an organization's budget and strategic goals is key to staying on track. From budgeting wisely to optimizing resource allocation, keeping a keen eye on the bottom line ensures the system's infrastructure remains both effective and economical in the long run. Additionally, a global information system infrastructure needs to be scalable to accommodate changing needs and requirements. Anticipating future growth and capacity needs is important for staying ahead of the curve. From expanding storage capacity to accommodating increased data traffic, having the flexibility to scale a global information system infrastructure ensures that an organization is ready for whatever comes its way.

Building Versus Outsourcing Global Information Systems

The decision to build or outsource (or buy) a global information system is an important one in modern business operations. Imagine that a multinational e-commerce company is seeking to expand its online sales operations across different countries. The decision of whether to develop a custom system or to purchase a pre-built solution to manage its global operations can have far-reaching implications on the organization. It is important to assess the company's existing information technology and information system infrastructures and identify which current or external systems can be integrated with a new global information system. This can help to reduce costs, improve efficiency, and avoid duplication of efforts. For example, a transportation system could be integrated with a global weather system to improve delivery planning, optimize resource allocation, and enhance customer satisfaction. By anticipating potential disruptions and making adjustments, companies can minimize delays and ensure timely deliveries.

As businesses navigate this decision-making process, they must carefully weigh various factors to determine the most suitable approach and to ensure alignment with organizational objectives. When considering building a system in-house, an organization should consider these questions:

- In addition to build costs, how much will integration, implementation, training, and ongoing maintenance cost?
- Can the company absorb the time it will take to build an in-house system, or are there time-to-market considerations that may become a competitive disadvantage?
- Does the business have adequate in-house expertise and resources to develop, implement, and maintain an in-house system?
- Are there intellectual property concerns that would be best protected by building a proprietary system?

Systems that are outsourced through a vendor or purchased outright require these considerations:

- How much value will the company derive from a vendor's expertise and services to implement and maintain an outside system?
- Are the system's preset features sufficient, and if not, to what extent can the system be tailored to meet specific needs?
- What reputation do potential vendors have in terms of reliability, maintenance services, and technical support?
- Will a purchased system be compatible with and integrate smoothly into existing company systems?

For any of the options, the business should consider these important questions:

- What are the year-over-year cost outlays of building versus purchasing or outsourcing?
- Does one option or the other offer an advantage in terms of future scalability requirements and the flexibility to adapt to changing business needs and technological advancements?
- Will the migration of data into the new system be a smoother and better transition with one option over the other?
- How easily will the system comply with data protection regulations, industry standards, and the security measures needed?

11.2 Global Information Systems Business Models, Logistics, and Risk Management

Learning Objectives

By the end of this section, you will be able to:

- Identify different types of global e-business models and enterprise strategies
- Describe logistics issues, models, and strategies
- Explain risk management and mitigation strategies associated with global data and systems sharing

As technology has transformed international business operations, e-business has become a vital tool, along with robust logistics processes and risk mitigation for the global stage. In the global marketplace, information systems are revolutionizing how these processes are handled, shaping the future of global organizations and helping them use technology to be more efficient and competitive throughout the world.

Global E-Business

A **global e-business** refers to the use of electronic communication and digital technologies to conduct business on a worldwide scale. It encompasses a wide range of activities including online sales, marketing, customer service, and collaboration with partners and suppliers across the globe. Global e-business has become increasingly important in today's digital economy, enabling organizations to reach customers and markets beyond their traditional geographical boundaries.

The shift to global e-business has revolutionized how companies operate. Businesses can now reach new markets and expand their customer base, streamline internal processes with online tools, and offer enhanced customer experience through global support and personalized online interactions. Consider a sports apparel company looking to compete on a global scale. Without e-business, they have limited market opportunities as they are reduced to selling in physical stores only, restricting their customer base to their domestic market, and limiting their brand awareness to their local market. With an e-business model, they can launch an online store, reach new customers worldwide, and establish their brand as a global player.

Online platforms enable businesses to operate around the clock, catering to different time zones and increasing sales opportunities. E-businesses often have lower overhead costs compared to brick-and-mortar operations as they save on expenses like rent, utilities, and on-site staff. E-business equips companies to compete effectively, streamlining operations, reaching new markets, and building a strong global brand in today's global marketplace.

Types of E-Business Models

An **e-business model** refers to the strategies and structures that businesses use to operate and generate revenue online. Table 11.1 outlines some of the primary e-business models. Each model leverages the connectivity and reach of the internet to create value and drive revenue.

Type	Description	Examples
Business-to-consumer (B2C)	Businesses sell products or services directly to consumers	Amazon, Zappos
Business-to-business (B2B)	Businesses sell products or services to other businesses	Salesforce, Smartsheet
Consumer-to-consumer (C2C)	Consumers sell products or services to other consumers, often facilitated by a third-party platform	eBay, Craigslist
Consumer-to-business (C2B)	Consumers offer products or services to businesses	Freelancer platforms like Upwork, and crowdsourcing platforms like 99designs
Business-to-government (B2G)	Businesses provide goods or services to government entities	Military equipment suppliers, construction companies
Government-to-business (G2B)	Government entities provide services or information to businesses	Trade licenses, public-private partnerships
Government-to-consumer (G2C)	Government entities provide services or information directly to consumers	Tax filing portals, driver's license services

Table 11.1 Types of E-Business Models These e-business models can be used independently or in combination, depending on the business strategy and market needs.

Global Enterprise Strategies

A **global enterprise strategy** is a comprehensive plan outlining how an organization will achieve its goals and objectives in a global marketplace, or the road map to an organization's success. Developing and implementing global enterprise strategies involve creating comprehensive plans that align with an organization's overall goals and objectives while considering the complexities of operating in a global environment. Effective global enterprise strategies are important for companies seeking to expand their operations and achieve success. Examples of companies with global enterprise strategies include Coca-Cola, Toyota, Microsoft, McDonald's, and Apple.

By developing and embracing innovative global strategies, organizations can unlock growth, navigate complexities, and thrive in today's interconnected world. Strategies might include the following:

- reaching out to new customers and revenue streams beyond domestic borders
- tapping into a global pool of talent, capital, and raw materials
- spreading operations across regions to mitigate economic and political risks
- gaining a global advantage through increased footprint and brand recognition
- sparking creativity by accessing diverse ideas and best practices worldwide
- establishing a strong, consistent brand identity across international markets
- expanding responsibly, considering environmental and social impacts

To implement a successful global enterprise strategy, an organization should proceed through these steps:

1. Complete a thorough analysis of the global business environment. This includes examining market trends, competitor strategies, regulatory requirements, and cultural factors.
2. Create clearly defined SMART (specific, measurable, achievable, relevant, and time-bound) objectives for global expansion.
3. Outline the specific actions required to achieve the organization's goals and incorporate the environmental analysis and objectives. Include details on employing market entry methods, managing cultural differences, addressing regulatory requirements, and building a strong global brand.
4. Determine the resources needed. These resources include financial capital, human resources with international expertise, and technological infrastructure to support global operations.
5. Assemble a diverse and talented team to execute the global enterprise strategy. This team should include individuals with expertise in international business, marketing, finance, operations, and other relevant areas, depending on the specific industry and target markets.
6. Measure key performance indicators such as market share, revenue growth, and profitability to assess the effectiveness and the progress of the strategy. Based on ongoing monitoring and evaluation, adjustments to the global enterprise strategy may be necessary. This might involve revising the market entry approach, realigning resource allocation, or refining product offerings to better meet the needs of global customers.

LINK TO LEARNING

The Strategy Institute is an organization that offers certifications for global information systems professionals (https://openstax.org/r/109GISCert) and provides other resources to help these professionals excel.

Global Logistics

The process of **global logistics** involves planning and managing the international transportation of goods to their destination. Global logistics is how clothing, shoes, medications, health products, or food can be ordered online and delivered to you a few days later. Global logistics entails detailed planning of how goods will be transported, what routes to take, and how to navigate customs regulations around the world. It considers the transportation mix (air, land, and water means) needed for the efficient movement of goods, and factors including cost, speed, and cargo type. It ensures the right amount of stock is in the optimal places with the goals of avoiding stock-outs and minimizing storage costs. It uses technology to track shipments, manage inventory, and ensure smooth communication across the supply chain.

Types of Logistics Models

Organizations employ different logistics models to efficiently manage the flow of goods, information, and resources. These models each offer distinct advantages and come with their own set of challenges. Choosing a suitable model depends on various factors, including the nature of the business, customer demand patterns, geographical reach, and cost considerations. Three common types of logistics models are third-party, just-in-time, and hub-and-spoke.

Third-party logistics (3PL) involves outsourcing logistics operations to a third-party service provider. Outsourcing can reduce operational costs by leveraging the provider's established networks and economies of scale. These vendors manage transportation, warehousing, distribution, and other logistics-related activities on behalf of the company. Providers of 3PL bring specialized knowledge and expertise, helping businesses optimize their supply chain. They also offer flexibility in scaling operations up or down based on fluctuations in demand without significant capital investment from the business using their services. Keep in mind that heavy reliance on a third-party provider can pose risks if the provider faces issues or disruptions.

Just-in-time (JIT) logistics focuses on minimizing inventory levels by receiving goods only as they are needed in the production process. This model strives to reduce costs and increase efficiency by lowering inventory levels, reducing storage costs, and minimizing waste from unsold or obsolete products. JIT offers streamlined operations, and reduced lead times can enhance supply chain efficiency, plus it promotes responsiveness to market demand, reducing excess stock. However, JIT is highly sensitive to supply chain disruptions, and delays from suppliers can halt production.

Hub-and-spoke logistics uses a central hub (distribution center) to consolidate and distribute goods to various spokes (destinations). Centralizing distribution can lead to significant cost savings in transportation and warehousing. Consolidation at the hub allows for efficient sorting, routing, and scheduling of deliveries, allowing expansion of networks and increased volumes. Managing a hub and spoke network requires sophisticated planning and coordination to ensure timely deliveries.

Why Use a Global Logistics Information System?

The implementation of a global logistics information system offers a compelling solution to several business problems. A **global logistics information system (GLIS)** is designed to manage and track the flow of goods across international borders, encompassing all aspects of a global supply chain. Imagine the transformative potential of possessing real-time visibility into the entirety of the supply chain. This includes both a comprehensive inventory overview and the precise location of every shipment in transit. Such transparency empowers a proactive approach to problem-solving and facilitates the formulation of informed decisions based on the most current data available.

The benefits of a GLIS extend far beyond mere visibility. It optimizes transportation routes to minimize costs and delivery times and automates repetitive tasks, minimizing human error and streamlining operational workflows. By providing accurate delivery estimates and proactively communicating potential delays, a GLIS empowers an organization to become a customer champion. A GLIS equips organizations with the agility necessary to adapt to the ever-evolving market landscape and seamlessly scale operations in support of global expansion. The consequence of these improvements is a leaner and more cost-effective logistics operation with a reduced risk profile. This is achieved through improved supply chain visibility, robust security features that safeguard sensitive data, and the ability to leverage data-driven insights to optimize decision-making across the entire logistics spectrum.

Global Supply Chain Management

Imagine you are managing the global supply chain for a company that designs cutting-edge athletic wear. The framework of global supply chain management keeps this global operation running smoothly. It encompasses everything from the first stitch to the final delivery, across international borders. The process of **global supply chain management (GSCM)** involves the planning, coordination, and optimization of the flow of goods, information, and finances across international borders to meet customer demands. It involves managing the entire supply chain from sourcing raw materials to delivering finished products to end customers, taking into account factors such as global sourcing, production, distribution, and logistics.

Types of Supply Chain Management Models

Choosing the right supply chain model is critical for businesses. It can affect everything from cost control to risk management and brand reputation. Table 11.2 shows six common models that organizations utilize based on the best fit for the company. There's no one-size-fits-all model, and selecting the right one depends on the specific industry, products, and business goals of the organization.

Supply Chain Management Model	Description	Businesses Best Suited For	Advantages	Disadvantages
Continuous flow	Streamlined operations with minimal waste	Industries characterized by stable demand and production patterns	Fits ideally with the production of standardized goods	Is inflexible and therefore less suitable for dynamic markets with rapidly evolving consumer preferences
Fast chain	Expeditious delivery of trend-driven products to market, capitalizing on short-lived consumer interest	Businesses operating in environments with short product life cycles, such as the fashion industry	Fosters competitiveness	Necessitates a high degree of adaptability and can be susceptible to disruptions in the supply chain
Efficient chain	Prioritization of efficiencies and cost reduction	Highly competitive industries with tight profit margins	Offers meticulous production forecasting to ensure minimal waste and optimal resource utilization	Is vulnerable to disruptions and requires accurate forecasting
Agile	Handling of expensive specialty goods	Businesses dealing with high-value, specialty products that demand precise handling	Utilizes premium pricing	Requires expertise in product transportation and handling

Table 11.2 Supply Chain Management Models Organizations should consider their strategic business goals, and the pros and cons of different models, when selecting a supply chain management system.

Supply Chain Management Model	Description	Businesses Best Suited For	Advantages	Disadvantages
Custom configured	Combining elements of both agile and continuous flow models	Companies engaged in prototype design and low-volume, customized production	Facilitates tailoring products to specific customer needs	Often necessitates a significant financial investment in customization processes
Flexible	Scales to fluctuating supply chain needs	Businesses grappling with variable demand patterns throughout the year	Allows for scaling production up or down in response to market fluctuations, minimizing stocking risks	Carries potential for increased complexity and challenging coordination

Table 11.2 Supply Chain Management Models Organizations should consider their strategic business goals, and the pros and cons of different models, when selecting a supply chain management system.

Effective Supply Chain Management

Managing the supply chain effectively involves overseeing processes such as sourcing, procuring, producing, and delivering goods and services to customers while optimizing costs, quality, and delivery times. Supply chain managers need to develop strong relationships with suppliers as well as communicate regularly, share information, and collaborate with partners to ensure timely delivery of high-quality goods and services. To align production and inventory levels with customer demand, reducing stock-outs and preventing excess inventory, companies need to consider historical data, evaluate market trends, and assess customer insights.

Managing costs is also a critical component of effective SCM. This includes using inventory management practices to minimize holding costs while ensuring product availability that can meet customer demands. Risk management is another important component of effective SCM, allowing for identification of potential risks and supply chain disruptions in order to minimize their impact. One area that cannot be overlooked is the use of performance indicators to monitor and measure supply chain performance so that areas of improvement can be identified and addressed.

Challenges of Global Risk Management

Understanding global enterprise risk management (ERM) is essential for businesses working internationally. For example, Uber uses a system for dynamic pricing, or surge pricing, which changes fare prices based on factors like where riders and drivers are, traffic conditions, and past data.[13] This system helps Uber manage supply and demand. By adjusting prices in real time, Uber makes sure riders can get a ride when they need one and encourages drivers to work in busy areas. However, managing this system globally comes with challenges like ensuring data accuracy and following different regional laws.

The importance of developing and implementing effective strategic and global ERM strategies boils down to two key concepts: proactive protection and sustainability. Enterprise risk management helps to proactively identify and mitigate global threats, safeguarding an organization’s reputation, building resilience in a volatile world, and ensuring avoidance of costly mistakes. Informed decision-making, optimized resource allocation,

13 Rohan Whitehead, “How Uber Utilises Data Science,” Institute of Analytics, May 30, 2024, https://ioaglobal.org/blog/how-uber-utilises-data-science/

and a competitive edge all stem from a strong ERM strategy that fosters sustained success.

Developing and implementing a strategic and global ERM strategy is essential for success, but it's not without its hurdles. Here's a breakdown of the key challenges and considerations:

- Gaining a comprehensive view of risks across a global organization: Data silos, cultural differences in reporting, and complex supply chains can hinder risk identification and assessment.
- Standardizing risk management practices across diverse geographical locations: Differences in regulations, languages, and risk tolerances can lead to inconsistencies in how risks are identified, assessed, and managed.
- Failing to consider cultural differences can lead to misinterpretations and ineffective risk mitigation strategies: Communication styles, legal frameworks, and risk perceptions can vary greatly across regions.
- Implementing a global ERM program requires dedicated resources like personnel, technology, and budget allocation.
- Securing buy-in from all levels of leadership and employees is crucial for successful system implementation.

By acknowledging these challenges, organizations can develop a robust and effective global ERM strategy that protects their operations and fosters long-term success in today's interconnected world. For example, in 2017, global shipping giant Maersk fell victim to a cyberattack perpetrated by the NotPetya malware.[14] Maersk utilizes a complex global information system to manage its vast network of shipping containers, ports, and logistics across the globe. The NotPetya attack, disguised as a ransomware, infiltrated Maersk's global information system and wreaked havoc. Terminals closed down, shipping schedules were disrupted, and communication between locations became nearly impossible. This resulted in significant financial losses and delays for Maersk and its clients. Moreover, the attack potentially exposed sensitive information within the system, such as customer data, shipment details, and internal communications. The Maersk attack serves as a reminder of the importance of robust security measures within global information system supply chain management.

11.3 Culture in Information Systems and Global Information Systems Teams

Learning Objectives

By the end of this section, you will be able to:

- Describe the concept of culture and its impact on organizations and information systems
- Explain the role of culture on technology adoption and use
- Describe global information system teams
- Explain what a cross-functional enterprise means to information systems

Culture is a set of rules and beliefs that shape people's thinking and attitudes. It is important to understand cultural differences and their importance in making technology work well in different situations. Culture affects technology adoption and can influence whether people embrace a new technology or are reticent toward change. For example, a global company might introduce a new global information system to employees in different countries. In some cultures, there might be a preference for hierarchical decision-making, while in others, a more collaborative approach might be favored. Understanding these cultural differences is essential for ensuring that the global information system is implemented effectively and aligns with local cultures.

The Impact of Culture on Organizations and Information Systems

Culture influences the values, norms, beliefs, and behaviors of individuals and organizations and plays an

14 Jacob Gronholt-Pedersen, "Maersk Says Global IT Breakdown Caused by Cyber Attack," *Reuters*, June 27, 2017, https://www.reuters.com/article/technology/maersk-says-global-it-breakdown-caused-by-cyber-attack-idUSKBN19I1N5/

important role in shaping the way technology is developed, implemented, and utilized in a company. Imagine an organization with leaders who foster a culture of innovation and risk-taking. Employees are encouraged to experiment with new ideas and embrace failure as a learning opportunity. What type of employee do you think this company is looking to hire? Someone who values stability and prefers well-defined processes? Or someone who is willing to take risks and experiment?

A broad and intricate concept, **culture** encompasses the beliefs, behaviors, customs, values, norms, symbols, and practices shared by a group or organization. Culture defines that group's way of life, shaping their perceptions, interactions, and understanding of the world, including their approach to technology and innovation. Culture is not static, but dynamic and ever-evolving, influenced by historical, social, economic, and environmental factors.

An **organizational culture** refers to the shared values, beliefs, and norms that influence how people interact, work together, and make decisions within an organization. It develops through shared experiences, leadership styles, policies, and workplace practices (Figure 11.6). Organizational culture is critical in how new technologies are perceived, adopted, and integrated into workflows. A culture that values innovation and adaptability is more likely to embrace technological changes, while a more risk-averse culture may resist them.

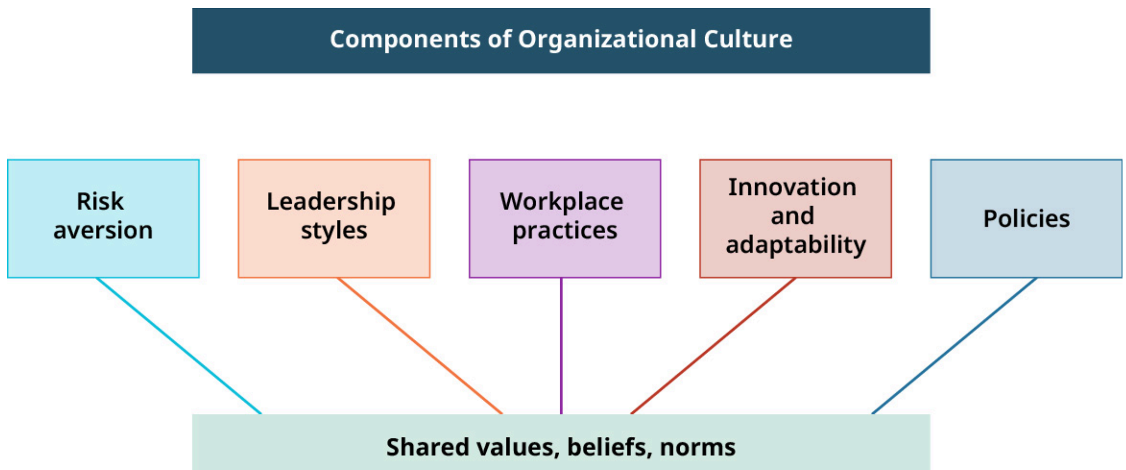


Figure 11.6 Organizational culture can impact how an organization does business, especially when that culture is different from other global businesses or varies across a single organization's locations. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

LINK TO LEARNING

Learn more about types of organizational culture (https://openstax.org/r/109OrgCulture) in this article.

A **personal culture** encompasses a person's unique experiences, beliefs, and personality traits that affect how they perceive and engage with their environment. An individual's history, social influences, education, religion, and reflections shape personal culture, which in turn can influence a person's interactions with technology, openness to new tools, and readiness to adapt to technological changes. Personal attitudes toward technology can affect enthusiasm and proficiency in using new systems. Some of the significant ways that culture typically impacts organizations include the company's and individuals' values and beliefs, norms and practices, power dynamics, and approaches to decision-making and planning.

At the personal level, values and beliefs impact attitudes toward digital privacy, data security, and innovation. For example, an individual's belief in the importance of privacy may influence their preferences for secure communication channels within information systems. Similarly, an organization's values regarding transparency, efficiency, and customer centricity inform their technological strategies and approaches to IS implementation. These values shape organizational culture, driving technological initiatives and shaping the digital environment in which individuals operate.

Norms and practices establish the rules and expectations regarding appropriate behavior. These norms may include personal conduct in the workplace, such as punctuality or communication etiquette, and within a global information system, these norms may include guidelines for online communication, data privacy practices, and technology usage. For organizations, norms may encompass policies and procedures governing employee behavior, teamwork, and decision-making processes. Norms may also govern IT security protocols, data management procedures, and collaboration practices within global information system platforms.

Power structures and dynamics can influence access and control within information systems. While some colleagues might prefer flat or shifting structures, others may appreciate a more hierarchal approach. Some employees prefer working as a team, while others prefer working alone. In organizational cultures with hierarchical power structures, access to IT might be restricted to certain groups, while more egalitarian organizational cultures might strive for wider access. For instance, in some organizations with clear hierarchies and those in power having more control and decision-making authority than others, only senior management might have access to certain data systems. In an organizational culture that values creative input from people at all levels, access might be more broadly distributed. The benefit of limited access to data systems for senior management is greater control and security, but the drawback is that it may slow decision-making and reduce employee empowerment. In more egalitarian cultures, broader access allows for faster decision-making and increased collaboration, but it may pose challenges in maintaining data security and control.

Decision-making and planning approaches will also vary. More often than not, different perspectives lead to creative solutions and collaboration enhances communication skills within the team. Keep in mind that misunderstandings can happen when people don’t appreciate or respond thoughtfully to these differences.

Understanding organizational cultural dimensions is key to fostering inclusive design, promoting effective collaboration, and ensuring that information systems serve the diverse needs of the global business community. The cultural iceberg model, shown in Figure 11.7, explains how both visible and hidden cultural elements impact the use of information systems within an organization. Visible aspects (above the surface) include language, user interface preferences, and basic norms that can be easily adjusted, such as adapting interfaces to local languages. Hidden aspects (below the surface) involve deeper cultural values like privacy concerns, trust in technology, and decision-making processes, which can affect how technology and information systems are perceived and used.

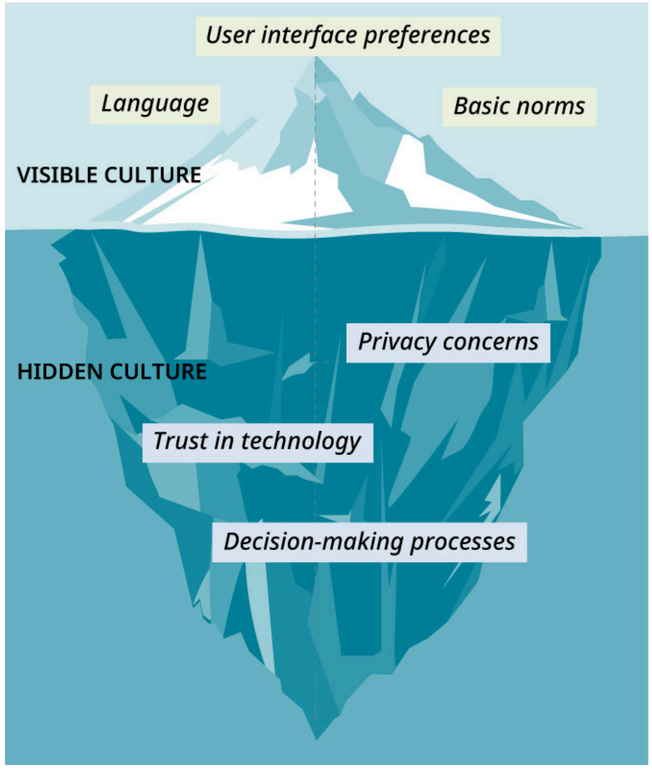


Figure 11.7 The cultural iceberg model demonstrates how some cultural elements are visible, while others remain more hidden. Both impact the use of the global information system within an organization. (credit: modification of work from *Psychiatric-Mental Health Nursing*. attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Culture and Technology Adoption

Organizations often encounter challenges when implementing new technologies, and these challenges can expand when technology is implemented across diverse cultural contexts. Communication barriers pose significant challenges and stem from differences in communication styles, languages, and norms across cultural boundaries. These barriers can impede effective collaboration and understanding among team members, hindering adoption.

Cultural resistance to change presents another obstacle, as individuals and groups may be hesitant to embrace new technologies that challenge established practices or norms. Cultural misunderstandings further complicate matters, as different interpretations of communication or behavior can lead to conflicts and breakdowns in cooperation. Addressing these challenges requires organizations to proactively foster cultural sensitivity, promote open dialogue, and develop strategies accommodating diverse cultural perspectives to foster successful adoption of technology.

Cultural Factors that Influence Technology Adoption

Technology adoption is influenced by a variety of factors, and they can vary significantly across different cultures. Understanding these is necessary for designing and implementing technology solutions that are culturally appropriate and effective. Companies should consider the role of culture—organizational, regional, personal, and so on—in their approach to how technology and information systems are adopted and implemented. This includes attention to differences like openness to innovation, collaboration and communication styles, language barriers, localization of information, and the digital divide.

Organizational cultures that prioritize innovation are more likely to embrace new technologies and invest in their implementation. Those valuing stability and tradition may resist change and be slower to adopt new systems or less open to workflow and process changes. Individuals who are early adopters and technology enthusiasts can drive cultural change within the organization, promoting a more innovative and tech-friendly environment.

Cultures encouraging collaboration and open communication facilitate the implementation of technologies requiring teamwork. In hierarchical cultures where decisions are made by senior management and passed down through limited communication channels, technology may be implemented without consulting end-users. This can result in resistance and poor adoption. In flat and participatory cultures, where users are actively involved in decision-making processes, technology is more likely to be embraced if changes include attention to employees' feedback and needs.

In a global organization, language barriers can lead to communication breakdowns that hinder data interpretation and decision-making. Technology design should be mindful of possible language barriers and the meaning of colors and symbols in the user interface. This includes menus, tooltips, and other textual elements being effectively adapted for user languages. Organizations should also ensure data labels, attribute names, and metadata reflect cultural nuances, and that users from different linguistic backgrounds can access and comprehend vital information seamlessly. Direct translations can fail to capture linguistic nuances. A system optimized for English-language acronyms might be meaningless in a French translation that uses different acronyms or in a language with a different alphabet. Consider the example of Google Maps in India, which supports transliteration of points of interest in ten local languages. This transliteration, which focuses on converting the sounds and characters of one language to another (rather than translation of words and their meanings), allows users to more effectively search for places within the software.[15]

Localization of information can create more value from systems. For example, incorporating local knowledge into geographic information systems (achieved through cultural visuals like signs and symbols, community mapping workshops, citizen science projects, interviews, and collaboration with local organizations) adds another layer of richness and context to the data. Local users can provide insights that may not have been captured in standard datasets. Integrating this information into systems enhances the relevance and accuracy of spatial information and can foster a stronger connection between the technology and the communities it serves.

Finally, companies should be aware of impacts of the digital divide. Cultures with better infrastructure, such as electricity and internet connectivity are more readily equipped to adopt technology than those with limited access. In a culture where technology has been more recently introduced, investment in training and support programs can lead to better user adoption of new systems.

LINK TO LEARNING

Cultural variations impact business practices and communication. In this TED talk, Valerie Hoeks discusses cultural differences in business (https://openstax.org/r/109TEDHoeks) and offers practical examples and strategies for navigating these differences effectively.

Identifying Cultural Barriers in Technology

Identifying cultural barriers in technology ensures successful implementation and user acceptance. There are various ways to identify cultural differences to understand how these factors influence attitudes, behaviors, and practices toward technology within an organization, including these methods:

- Conduct cultural assessments: Utilize surveys and questionnaires to gather information on attitudes and beliefs regarding technology. Focus groups and interviews with employees can be used to gather information about the perceptions of and concerns about technology.
- Analyze communication styles: Observe employees and use feedback mechanisms to identify differences

15 Tribune Web Desk, "Google Maps Improves Discoverability in Indian Languages," *The Tribune*, January 27, 2021, https://www.tribuneindia.com/news/science-technology/google-maps-improves-discoverability-in-indian-languages-204096/

in communication patterns and barriers.

- Skill assessment: Use assessments to evaluate current technological skills and literacy levels and to identify gaps and cultural factors that affect training.
- Evaluate the organizational culture: Use culture audits and surveys. Look at past technology implementations and analyze the lessons learned to identify recurring issues. Consider engaging experts to gain insights into cross-cultural communication and organizational behavior.
- Use pilot tests: Prior to adoption, technology can be pilot tested on a small scale to identify cultural barriers as well as gather detailed feedback from pilot participants to refine the adoption, implementation, and use of the technology.
- Use frameworks: Frameworks can be used by companies to identify and understand differences. For example, Hofstede's Cultural Dimension examines six factors—power, individualism, gender, uncertainty, time, and control—to understand culture in the workplace (Figure 11.8).[16], [17]

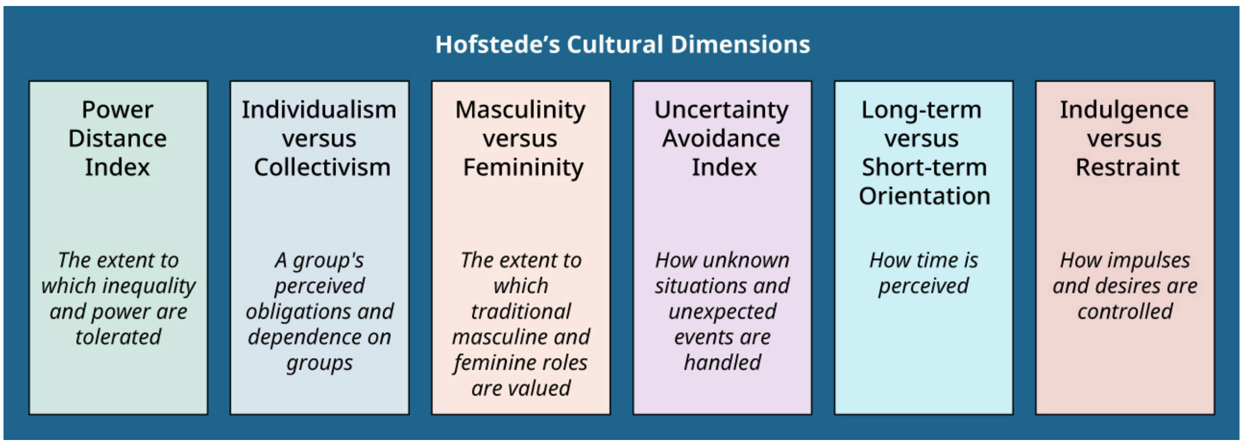


Figure 11.8 Hofstede's Cultural Dimensions can help analyze cultural differences within an organization. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Designing Culturally Appropriate Technology and Systems

Global information system development often involves teams that span multiple countries and cultures. For example, the International Space Station (ISS) represents an extraordinary global collaboration in the field of science and technology. Five space agencies, representing fifteen nations, have worked together to build and maintain the ISS.[18] Effective cross-cultural collaboration is essential for successful global information system development. This type of collaboration involves navigating and integrating diverse perspectives, values, communication styles, and practices that arise from cultural differences, as well as a commitment to building trust, communication, and collaboration across cultural boundaries. It is imperative that this collaboration is facilitated by senior leaders. Following are some strategies for effective cross-cultural collaboration:

- Foster inclusive leadership that recognizes and values the contributions of team members from diverse cultural backgrounds.
- Develop cultural awareness among team members to provide an understanding of the cultural values, norms, and communication styles of team members.
- Establish clear and open communication channels to facilitate understanding and collaboration. Use translation tools and supports to ensure proficiency in a common language.
- Encourage flexibility and a willingness to adapt systems development processes to accommodate different cultural preferences and practices.
- Develop and implement strategies for resolving conflicts that may arise due to cultural differences.

16 Geert Hofstede, "The 6-D Model of National Culture," accessed January 27, 2025, https://geerthofstede.com/culture-geert-hofstede-gert-jan-hofstede/6d-model-of-national-culture/
17 Charlotte Nickerson, "Hofstede's Cultural Dimensions Theory & Examples," *Simply Psychology*, October 24, 2023, https://www.simplypsychology.org/hofstedes-cultural-dimensions-theory.html
18 "Station Facts," National Aeronautics and Space Administration (NASA), accessed January 27, 2025, https://www.nasa.gov/international-space-station/space-station-facts-and-figures/

- Implement platforms that support diverse languages, multiple time zones, and various cultural contexts.

Understanding cultural influences is essential for designing technology that is culturally sensitive, inclusive, and effective in meeting the needs and preferences of stakeholders using the systems. Here is a list of key principles to follow:

- Research the cultural norms, values, and practices of your target users. Consider how these factors might influence how they will interact with the technology.
- Involve a diverse group of employees including differing cultures, genders, ages, abilities, and technical skills, throughout the design process. Gather their feedback on features, language, and overall usability.
- Use clear, culturally appropriate language in interfaces and instructions. Consider symbols, icons, and metaphors that will resonate with employees.
- Design technology that allows for customization. This could include different language settings, options for displaying information, or adapting to local cultural norms. For example, a global e-commerce business like Amazon.com allows users to customize their experience by selecting different language settings, adjusting currency preferences, and choosing regional product recommendations to match local shopping habits.
- Ensure the technology is usable by employees with varying levels of digital literacy. Consider creating clear interfaces, text-to-speech options, and support materials in multiple languages.
- Consider the ethical implications of the technology. This includes respecting user privacy, ensuring data security, and avoiding any form of cultural appropriation.

Global Information System Teams

Global information system teams play a critical role in organizations, especially in the context of cross-functional collaboration. These teams are responsible for developing, implementing, and maintaining information systems that support the organization's global operations. Global information system teams must collaborate closely to understand their requirements, align the system's strategies with business objectives, and ensure that the system's solutions meet the needs of all stakeholders.

An organization's **global information system team** is the group of professionals responsible for designing, implementing, managing, and securing the complex systems that enable the flow of information across international borders. Figure 11.9 shows the key roles in these teams.

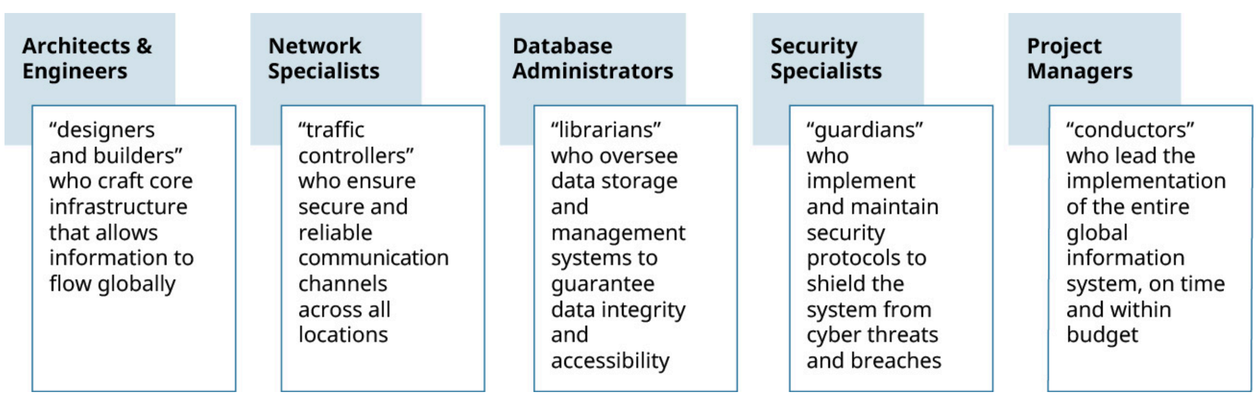


Figure 11.9 Global information system teams typically consist of members from different functional areas within the company—such as IT, finance, marketing, and operations—working together to achieve common goals. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

In terms of the technical management of global information systems and coordination with IT services, the global information system team should ensure it has roles for these functions:

- IT leadership: Sets the direction, allocates resources, and ensures IT aligns with business goals, including policies, standards, budgets, projects, and compliance.
- Regional IT: Manages IT operations and support in specific regions (infrastructure, user support, regional

projects, local regulations, culture).

- Infrastructure: Designs, deploys, and maintains the organization’s global IT infrastructure (networks, servers, data centers) for effective availability, performance, and security (cloud, resource optimization).
- Applications: Develops, deploys, and supports enterprise applications used globally (development, customization, life-cycle management, user support, integration, data integrity/security).
- Data governance and compliance: Ensures data management practices follow regulations and internal policies (data governance policies, data quality and integrity, privacy and protection, compliance audits).
- Security: Protects IT assets and data from cyber threats (security policies, audits, monitoring, incident response, security awareness training).

Since geographic information system teams are typically spread across various locations around the world, managing such diverse teams requires key strategies such as the following

- cultural awareness, where team members respect and navigate cultural differences
- use of videoconferencing, chat platforms, and project management software to keep everyone informed and aligned, considering time zone variations
- open communication, idea sharing, and feedback through collaborative tools
- defined team goals and roles that align with the organization’s vision statement
- acknowledgment of accomplishments and rewards for outstanding performance
- addressing of conflicts promptly and constructively, fostering open dialogue and seeking mutually agreeable solutions

Cross-Functional Enterprises

Global enterprises need to navigate complex markets and diverse customer needs, and this is where a cross-functional enterprise comes in. A **cross-functional enterprise** is an organization that breaks down departmental silos and fosters collaboration between different functions (such as marketing, finance, and IT) to achieve common goals. The most successful organizations abandon a siloed structure, where departments operate independently, and create a collaborative network where departments work together as a cohesive unit. This approach unlocks a range of benefits:

- Diverse teams often generate innovative ideas and solutions.
- Streamlined communication and collaboration eliminate redundancies.
- Teams quickly mobilize resources to address new challenges.
- Diverse perspectives can lead to well-rounded decisions.
- Opportunities for cross-functional work can boost morale.
- Enhanced efficiency, innovation, and agility fuel global expansion.

Cross-functional enterprises come in various forms, each with distinct characteristics and roles. Table 11.3 describes these structural approaches.

Enterprise Type	Description
Matrix organization	These types of organizations feature a dual reporting structure where employees report to both a functional manager (such as IT, marketing, or finance) and a project or product manager. This enables efficient resource and expertise allocation across functions for specific projects.
Network organization	These organizations have a flexible and decentralized structure where employees, partners, and suppliers collaborate in a networked environment, often using technology to facilitate communication and collaboration across functions and locations.
Global enterprise	These enterprises operate across multiple countries and regions, navigating diverse cultural, regulatory, and market environments. They use cross-functional teams to manage global operations, address local market needs, and ensure regulatory compliance.
Project-based enterprise	These enterprises focus on delivering projects or initiatives with a prioritization on project management to complete projects on time, within budget, and to quality standards They use cross-functional teams—temporary groups from different functional areas formed to work on specific projects or solve particular problems—which allows leverage of diverse skills and expertise to achieve their objectives.
Agile organization	These organizations adapt quickly to change and customer needs, using cross-functional teams to develop and deliver products and services in short, iterative cycles, allowing rapid response to market changes and customer feedback.

Table 11.3 Types of Cross-Functional Enterprises By fostering collaboration across departments, cross-functional enterprises empower global organizations to navigate the complexities of the international marketplace and achieve sustainable success.

Managing cross-functional organizations requires a focus on building strong teams with diverse skill sets and clearly defined roles. Fostering open communication and shared goals is crucial, alongside effective leadership that navigates cultural sensitivities and resolves conflicts constructively. Investing in training, recognizing achievements, and implementing performance management empowers teams and unlocks their potential for driving global success.

Key Terms

cross-functional enterprise organization that breaks down departmental silos and fosters collaboration between different functions (such as marketing, finance, and IT) to achieve common goals

culture beliefs, behaviors, values, norms, symbols, and practices shared by a group or organization

data interoperability ability of diverse data systems or formats to exchange, integrate, and interpret data accurately and efficiently

e-business model strategies and structures that businesses use to operate and generate revenue online

geographic context impact of location on operations

global e-business use of electronic communication and digital technologies to conduct business on a worldwide scale

global enterprise strategy comprehensive plan outlining how an organization will achieve its goals and objectives in a global marketplace

global information system intricate network of hardware, software, data, and telecommunications infrastructure that enables information collection, storage, management, processing, analysis, and dissemination worldwide

global information system infrastructure foundational framework of hardware, software, data storage, network, and cloud-based services that supports global information system operations within an organization

global information system team group of professionals responsible for designing, implementing, managing, and securing the complex systems that enable the flow of information across international borders

global logistics planning and managing the international transportation of goods to their destination

global logistics information system (GLIS) system designed to manage and track the flow of goods across international borders, encompassing all aspects of a global supply chain

global supply chain management (GSCM) planning, coordinating, and optimizing the flow of goods, information, and finances across international borders to meet customer demands

interoperability standard guideline, protocol, or specification that enables different systems, technologies, or platforms to communicate, exchange data, or work together seamlessly

needs assessment gathering and analyzing data to identify and evaluate the current state, areas for improvement, and interventions needed to get to a more improved state

organizational culture shared values, beliefs, and norms that influence how people interact, work together, and make decisions within an organization

personal culture a person's experiences, beliefs, and personality traits that affect how an individual perceives and interacts with their environment

predictive analysis use of data, specifically statistical algorithms, to help organizations identify patterns and make predictions that will enhance the operational results

resource utilization efficient and effective allocation and management of resources such as time, money, materials, or personnel to achieve desired objectives or outcomes

spatial analysis process of examining patterns, trends, and relationships within geographic data to gain insights and make informed decisions about spatial phenomena

Summary

11.1 The Importance of Global Information Systems

- Global information systems support the standardization of business practices and workflows, ensuring consistency and efficiency across global operations. They are crucial in facilitating global connectivity, supporting informed decision-making, enhancing operational efficiency, breaking geographical barriers, nurturing innovation and creativity, and fostering global citizenship.
- Global information systems enable organizations to integrate their operations across locations, facilitating

centralized data management, streamlined processes, and operational consistency.
- Anticipating future trends and outcomes, global information systems allow organizations to create scenario models and conduct predictive analysis to assess the potential impacts of various strategies and courses of action.
- The global information system infrastructure relies on a variety of hardware and software components to function, including computers, workstations, routers, and peripherals, such as cables, printers, and scanners, as well as servers, storage devices, and end-user devices necessary for processing and storing data. Software components include operating systems, communication protocols, and GIS applications and tools needed to create, edit, analyze, and share data effectively.
- Building a robust global information system infrastructure requires understanding the organization's needs, defining clear objectives, assessing technology needs, selecting the right technologies, designing the infrastructure, phasing implementation, providing training and ongoing support, providing continuous monitoring and maintenance, and soliciting feedback and making improvements.
- A global information system enhances BI by using geographic information systems for spatial data analysis, which leads to improved decision-making, enhanced operational efficiency, heightened competitiveness, refined strategic planning, and the identification of new business prospects.

11.2 Global Information Systems Business Models, Logistics, and Risk Management

- E-business models allow businesses to reach new markets, streamline operations, and offer enhanced customer experiences.
- Developing a global organizational strategy is essential for companies seeking international success. Considerations include market analysis, SMART objectives, outlining actions to be taken, securing resources, and establishing a diverse team for execution. Monitoring and adapting the strategy based on performance indicators is crucial for long-term success.
- Global logistics involves meticulous planning for transporting goods internationally, considering factors like cost, speed, and regulations. Businesses can leverage different logistics to optimize their supply chains.
- Global supply chain management encompasses the entire flow of goods, information, and finances across international borders. Businesses can choose from various supply chain models to best suit their needs.
- Effective SCM helps businesses optimize costs, expand market reach, diversify suppliers, and adapt to market fluctuations.
- Strong risk management is crucial for organizations engaging in global operations and data sharing.

11.3 Culture in Information Systems and Global Information Systems Teams

- Culture shapes how people view and use technology. Personal and organizational cultures influence openness to new technology and adoption rates.
- It is important to evaluate cultural differences to support successful development, adoption, implementation and use of technology and systems.
- Cross-cultural collaboration is essential as successful global information systems development requires understanding and respecting cultural differences in communication, teamwork, and decision-making.
- Design technology that considers culture is imperative for organizations. User research, clear language, customizable features, and ethical considerations are necessary for culturally appropriate technology.
- Global information system teams design, implement, and maintain information systems that enable global operations to operate successfully.
- Effective global information systems teams require cultural awareness, clear communication, and efficient collaboration tools to successfully manage teams across borders.
- Cross-functional companies break down departmental silos and leverage diverse teams for better decision-making, innovation, and agility.

Review Questions

1. How does a global information system enhance global collaboration and surmount geographic obstacles?
   a. by eliminating physical barriers between nations
   b. by facilitating cross-border information exchange and communication
   c. by protecting access to data and information
   d. by focusing businesses' reach solely on one market
2. What is the primary role of global information systems in multinational enterprises and international groups?
   a. eliminating the need for communication among global teams
   b. fostering competition between different regions
   c. supporting innovation and collaboration across continents
   d. explaining growth and expansion opportunities
3. Which aspect of a global information system makes it instrumental in emergency response and disaster management?
   a. provides historical data on hazards and vulnerabilities
   b. eliminates the need for real-time information
   c. enables efficient coordination of emergency efforts
   d. substitutes for communication channels among responders
4. What sets global information systems apart from traditional information systems regarding their scope of operations?
   a. They support internal operations within a single organization.
   b. They offer advanced features for managing data across multiple organizations and geographic boundaries.
   c. They limit the need for managing structured data.
   d. They minimize the need for integration with external databases.
5. What feature of a global information system ensures compatibility among different global information systems, enhancing data exchange?
   a. scalability measurements
   b. communication protocols
   c. cloud computing services
   d. interoperability standard
6. What is the first step when designing a global information system infrastructure?
   a. defining clear objectives
   b. assessing technology needs
   c. understanding the organization's needs
   d. selecting the right technologies
7. Which feature of a global information system can help organizations improve decision-making, be more efficient, and identify new business prospects?
   a. supply chain management
   b. scalability
   c. spatial analysis
   d. data migration
8. Which of the following is not a benefit of e-business for global enterprises?
   a. increased brand awareness
   b. limited market expansion
   c. streamlined operations

   d. enhanced customer experiences

9. What is the primary focus of the just-in-time logistics model?
   a. minimizing inventory levels
   b. reducing transportation costs
   c. ensuring timely deliveries
   d. increasing storage capacity

10. How does a well-managed global supply chain benefit a company?
    a. reduced risk of data breaches
    b. outsourcing of customer service
    c. lowered production costs
    d. increased number of communication systems

11. What is a SMART objective for a global expansion strategy?
    a. increase brand awareness internationally
    b. expand into five new markets within two years
    c. improve customer satisfaction globally
    d. develop a global marketing plan

12. Why is strong risk management important for organizations engaging in global data sharing?
    a. avoid delays in project deadlines
    b. ensure data are used for marketing purposes
    c. minimize potential threats to data and systems
    d. simplify the process of sharing data

13. When designing a culturally sensitive system, what is the *least* important factor to consider?
    a. implementing a user-centered design approach involving target users
    b. translating content into local languages
    c. using the latest technology available
    d. adapting the system to be flexible and customizable

14. Culturally sensitive design requires ongoing efforts. Which of the following is the *best* way to ensure a system remains culturally appropriate over time?
    a. relying solely on the initial cultural research conducted before design
    b. implementing feedback mechanisms for users to suggest improvements
    c. translating the system into as many languages as possible
    d. avoiding any cultural references altogether

15. What is a primary responsibility of global information system teams?
    a. managing social media accounts
    b. designing and maintaining information systems for global operations
    c. overseeing marketing campaigns
    d. handling customer service inquiries

16. What is a key benefit of cross-functional teams?
    a. increased departmental competition
    b. improved communication and collaboration
    c. limited sharing of information
    d. slower decision-making processes

Check Your Understanding Questions

1. How does a global information system enhance decision-making processes in organizations?

2. How does a global information system contribute to cost reduction and customer satisfaction in global operations?
3. Explain the differences among the e-business models of business-to-consumer, business-to-business, consumer-to-consumer, and government-to-business.
4. What is the hub-and-spoke model of logistics? What are the benefits of this model, and what must organizations consider if they use it?
5. Which supply chain management model is most appropriate for highly competitive industries with tight profit margins? Why is this model the most appropriate for these types of businesses?
6. What legal and regulatory risks are posed by global data and systems sharing and how can these affect organizations?
7. Name at least three challenges of risk management.
8. How can a strong emphasis on hierarchy within an organizational culture hinder the adoption of a new collaborative technology?
9. Describe the importance of global information system teams in global enterprises.

Application Questions

1. How does the scope of operations differ between global information systems and traditional information systems, and what specialized features do global information systems offer for managing global operations?
2. You are a consultant advising a small clothing company that is looking to expand its business internationally. What are some key considerations related to e-business and global logistics that you would recommend they address?
3. Your company is facing increasing competition from emerging markets. To maintain a competitive edge, you've decided to implement a digital transformation strategy. Given your experience with global information systems, how would you leverage global information systems to support this digital transformation and enhance your company's competitiveness?
4. You are the CEO of a company that manufactures high-end athletic wear. You've identified a significant market opportunity in a developing country with a rapidly growing middle class. However, this country also has stricter regulations on labor practices and environmental sustainability compared to your current markets. Develop SMART goals to guide the global enterprise strategy for entering this new market.
5. How can global information systems be used to support sustainability initiatives within a global enterprise?
6. Discuss how global information system technology enhances supply chain management in real-world scenarios, and provide an example to illustrate its application.
7. Imagine you're tasked with designing a new global information system for a global company. The global information system will be used in offices located in both the United States (individualistic, low power distance) and Japan (collectivistic, high power distance). How might these cultural differences influence your design approach, and what challenges might you anticipate for user adoption in each location? Explain your answer.
8. An organization is considering implementing a global information system to improve data sharing and collaboration across their international offices. The company culture is one that values careful consideration and thorough review before making changes. How can this company navigate the potential conflict between their established culture and the fast-paced nature of implementing and utilizing a new

global information system worldwide?

12

Ethics, Sustainability, and Social Issues in Information Systems

Figure 12.1 People involved in planning, managing, and using information systems must carefully consider the ethical implications of balancing technological concerns with sustainability and social issues. (credit: modification of work "wocintech stock - 203" by WOCinTech Chat/Flickr, CC BY 2.0)

Chapter Outline

12.1 Ethics, Sustainability, and Use of Information Systems
12.2 Intellectual Property
12.3 Ethics of Artificial Intelligence Development and Machine Learning
12.4 Ethics in Health Informatics

Introduction

Have you ever faced an ethical dilemma at your workplace or in your academic studies? Do you get excited about the potential positive outcomes of new technology but also worry about possible negative impacts on society? How important is it that companies implement low-waste and environmentally aware practices? These questions touch on some of the concerns about ethics, social responsibility, and sustainability in the field of information systems.

At its core, information systems technology offers immense potential to transform society and enhance human welfare. But realizing this promise—in an ethical and socially responsible manner—requires establishing thoughtful governance and aligning innovations with core human and societal values. As information systems permeate our professional and personal spheres, ethical considerations around issues such as privacy, accountability, transparency, sustainability, equity, and human dignity become increasingly apparent. Proactive and holistic approaches to emerging technologies can steer this progress toward moral paths that uplift society both today and tomorrow.

12.1 Ethics, Sustainability, and Use of Information Systems

Learning Objectives

By the end of this section, you will be able to:

- Understand ethical perspectives and how they apply to information systems
- Define sustainability of information systems
- Explain the ethical impact of information systems on society

One of the most critical issues in the field of IS is determining how you will plan, use, and manage information systems and technological systems that you encounter. The values and principles that guide life decisions and experiences are known as **ethics**. Properly understood, almost nothing could be of greater importance. In terms of information systems, ethical considerations include both sustainability and the social impact of IS.

Normative Ethical Perspectives

Each day, individuals and organizations must make decisions. To determine the best action to take in a specific situation, decision-makers usually consider whether an action is an efficient and effective way to reach a desired outcome. They also think about the resources, such as time and money, needed to achieve a goal. And, whether conscious of it or not, most decision-makers consider whether an action is ethical. While ethics can be approached from many different viewpoints, humanity generally tends to rely on three perspectives to guide decisions and actions—utilitarianism, deontology, and virtue. All three perspectives are considered normative theories because their purpose is to provide guidance on how a person *ought* to act. This is contrasted with descriptive theories, which are based on explaining how individuals actually do act. These perspectives, which may also be referred to as theories and approaches to ethics, focus one's attention on different components of the decision-making process; this is why they can sometimes arrive at different conclusions. A utilitarian approach focuses on the consequences of an action, deontology focuses on the action taken, and virtue ethics focuses on how an individual's character influences the actions they take. Each of these approaches can help you to understand how people ought to behave in a given context.

Utilitarianism

The concept of **utilitarianism** describes a normative ethical theory holding that the morally correct course of action is the one that maximizes utility and happiness for the greatest number of people. The roots of utilitarianism are generally traced to the English philosopher Jeremy Bentham (1748–1832) and the name of this theory derives from the utility of the actions taken. What are the consequences, and how are those consequences valued? For example, if you take your friend's apple without permission, you have gained an apple but likely lost your friend's trust. Is it more useful to have your friend's trust or their apple?

The simplest conceptual understanding of this theory is that people should be guided in their ethics, their choice of action, by the following principle: Create the greatest good for the greatest number of people. Over time, utilitarianism has become connected with capitalism and Adam Smith (1723–1790), often referred to as the founder of modern capitalism. This makes sense since the goal of capitalism—maximizing economic production and benefits—can be regarded as a utilitarian goal. With utilitarianism focused on maximizing the greatest good, one can understand why this is the dominant ethical theory applied in business today. Consequentialism, the broader name given to this ethical approach under the utilitarianism theory, is a person's determination of whether the actions they take are ethical or not based on the consequences of those actions.

While utilitarianism is popular among business professionals, in practice, their actions do not always reflect its proper application. For example, imagine that you work for a company that manufactures a smart coffee maker, and the market share percentage of your company's top competitor is twice as much as your company's market share. Your supervisor asks you to reverse engineer the competitor's smart coffee maker and use the information gained to improve your company's product. A year later, your company's market share doubles, while your competitor loses market share. Although this action may have maximized the greatest good for your company, it hurt your competitor.

In the world of business, including areas focused on information systems and technology, it can be challenging to apply utilitarianism appropriately. First, imagine the difficulty in truly determining what the proper course of action would be in trying to figure out whether certain actions would create the greatest good for the greatest number of people. What *is* good? How do we know if the actions maximize the quantity of that good for the greatest number of human beings on the planet? What is the context within which we measure this good? Is it in the people in an organization, those in a community, the individuals in a particular society, or all human beings that inhabit the entire planet?

These are the key difficulties involved in properly applying the principles of utilitarianism. Also, one can be sympathetic to the plight of people operating within the business context when they transform the difficult-to-measure variables of "good" and "people" into the much more measurable (and generally desirable) variables of "money" and "stakeholders." There are many conflicts of interest that a business can face when trying to operate for the good and make a profit at the same time. As a result, in application, this can lead to unethical outcomes as measured by the original intent of this theory.

Another difficulty in properly applying utilitarianism is the misunderstanding that the greatest good is associated with majority rule. For instance, suppose in a class of 100 students, the class took a vote, and ninety-nine students decided to make one student responsible for taking all the notes, translating them electronically, organizing them, and distributing them to the other ninety-nine students. As a result of this decision, the remaining ninety-nine students would do nothing but wait for the notes to arrive prior to the exam. The majority ruled in this instance, and this led to 99 percent of the class doing no work in preparation for an exam that was supposed to serve as a measure of everyone's learning of the course material. Using the concept of majority rule, one could make the argument that this is an appropriate application of utilitarianism.

But, in this case, is majority rule an ethical approach to utilitarianism? Did this decision result in the greatest good for the greatest number of people? Of course not. Is goodness simply measured as the least amount of overall class effort needed to obtain the highest average grade in a class? Is it good that 99 percent of the students did not engage with the course material throughout the semester, or that they were not able to take in the teachings from the course and put them into practical use? Is this good for each individual student? Is this good for the university from which the student graduates whose students enter society unable to effectively perform the abilities that class was supposed to teach? Is this good for the well-being of the society within which those individuals operate? Questions such as these reach toward the ideal nature of goodness at the heart of utilitarianism.

Deontology

The concept of **deontology** describes a normative ethical theory that focuses on the inherent rightness or wrongness of actions themselves, as opposed to the consequences of those actions, following the premise of treating others the way you would like to be treated. The school of deontology is usually attributed to philosopher Immanuel Kant (1724–1804). Its name comes from the Greek word for "duty," and it is often referred to as the duty-based approach. Kant's maxim is stated as such: Act only in accordance with that maxim through which you can at the same time wish that it becomes universal law.[1] The simplest interpretation of this is to only take an action if everyone else should also be able to do it. You may recognize this idea as the Golden Rule: Treat others the way you would like to be treated, or act toward others the way you would want others to act toward you. Expressed this way, deontology becomes clear: the action one takes is the focal point for whether the decision being made is ethical. For a deontologist, the consequences of your actions are irrelevant because it is impossible for you to truly know what all the consequences of your actions would be. However, you could know if your action was in alignment with a universal maxim that reflects a natural law.

Practical application of this theory often devolves into a discussion about what specific duties need to be followed (lying is wrong, physically injuring others is wrong) and the fact that exceptions lie on the fringes of the theory. To explore this, assume that you maintain the computer systems and personnel files for your company's human resources division. You receive a request for information about a former employee who was terminated. The employee is being considered for a new position but will not get the position if you reveal that the employee was terminated. Since you have access to the employee's personnel file, you know the details of the termination, and you are confident that the employee was terminated unfairly. Should you lie and say that the employee willingly left their position? Or should you tell the truth knowing that this will harm the employee because they will not get the job? The duty you intend to follow is not about particular types of actions; rather, it is about following the more general principle that applies to all actions. Namely, you should take only those actions that benefit yourself and your fellow human beings. The key is not to rationalize the type of rules to be followed but rather focus on the feeling it engenders when you take actions that are meant for the betterment of others as well as yourself.

Virtue Ethics

The approach of **virtue ethics** is based on the premise that there are virtues and ideals toward which each human being should strive to allow the full expression of their humanity to flourish. This approach can be traced back nearly 2,500 years to the people of ancient Greece, specifically to the philosopher Plato (427?–347 BCE), his teacher Socrates (469?–399 BCE), and his student Aristotle (384–322 BCE). As such, virtue ethics is the original normative ethical theory and the primary influence on humanity until the later development of deontology and utilitarianism. For over a century, virtue ethics was relegated to the background in favor of deontology and utilitarianism. However, there has been a resurgence of interest in this approach thanks in part to G. E. M. Anscombe's 1958 article, "Modern Moral Philosophy," in which she has been noted as having:

> increasing dissatisfaction with the forms of deontology and utilitarianism then prevailing. Neither of them, at that time, paid attention to a number of topics that had always figured in the virtue ethics tradition—virtues and vices, motives and moral character, moral education, moral wisdom or discernment, friendship and family relationships, a deep concept of happiness, the role of the emotions in our moral life and the fundamentally important questions of what sorts of persons we should be and how we should live.[2]

The earliest, most direct, and accessible source of virtue ethics is Plato. Plato taught that there were four virtues that one needed to embody to live an ideal life: Courage, wisdom, moderation, and justice. Courage can be understood as the ability to maintain the intent to do good in whatever actions you take. Wisdom is knowing the proper relationship among all things, so that one has developed the understanding to naturally take the action that generates the most good for self and others. Moderation, or temperance, is the control of one's instinctual fears and desires, their pains and pleasures, to operate in a more rational manner of thoughtful consideration. Justice is the alignment of your action with the ideal; the closer you are to the ideal, the more just your actions become.

Synthesis

Consider a scenario in which your company has been profitable but needs to cut costs to maintain long-term sustainability. The executive team proposes paying out large bonuses to themselves, citing that it's part of their compensation plan. However, the company also needs to lay off a substantial portion of its staff due to budget constraints. The executive team's actions can be reviewed through the concept of virtual ethics. For example, do their actions demonstrate the virtues of fairness and empathy? Were they compassionate for the employees they laid off in making their decision? Are the leaders acting with integrity, balancing their personal

---

1 Immanuel Kant, *Grounding for the Metaphysics of Morals: with, On a Supposed Right to Lie because of Philanthropic Concerns*, 3rd ed., trans. James W. Ellington (Hackett Publishing Company, 1993), 30.
2 Rosalind Hursthouse and Glen Pettigrove, "Virtue Ethics," *The Stanford Encyclopedia of Philosophy*, Winter 2022 Edition, eds. Edward N. Zalta and Uri Nodelman, (July 18, 2003, revised October 11, 2022), https://plato.stanford.edu/archives/win2022/entries/ethics-virtue

interests with the well-being of the larger community, including those who depend on the company for their livelihoods? A virtue ethics–based decision would involve the executives reflecting on the kind of people they want to be and how their actions align with virtues like honesty, integrity, and justice. They might decide, for instance, to forgo or reduce their bonuses, showing empathy for those losing their jobs and prioritizing the welfare of the broader community over their individual interests.

So how are these concepts—utilitarianism, deontology, and virtue ethics—applied in an information systems setting? To explore this, assume you work for a company that provides the technology to support Mobility as a Service (MaaS) for public transit systems. With MaaS, passengers access one interface and pay portal to plan and pay for a trip that includes multiple modes of transportation, such as bicycling, riding a bus, and riding a subway to reach their destination. You are part of a team brainstorming ways to market your company's MaaS technology to cities across the United States. The needs and resources of these cities vary greatly, providing disparate opportunities for your company to earn a profit. As you and your team explore options, you likely will be influenced by utilitarianism as well as deontology and virtue ethics.

From a utilitarianism perspective, your marketing plan should aim to increase access to MaaS in cities that will benefit the most, considering both immediate customer needs (such as more affordable transportation options) and long-term impacts (like reduced congestion and lower emissions). From a deontological perspective, how can you ensure that cities have an equal opportunity to purchase and take advantage of your company's MaaS technology? Your marketing plan would aim to provide equitable access for all customer groups because it is the right way to do business. How will virtue ethics guide your personal contributions to the discussion to help promote equality and the greatest good in your company's marketing plan, while also recognizing that your company wants to achieve a certain profit margin in sales of its MaaS technology? Balancing utilitarianism, deontology, and virtue ethics with goals such as profit maximization can be challenging. When people and organizations achieve that balance, they can attain positive results that help promote a fairer and more just society.

Systems Thinking and the DIKW Pyramid

A tool that aids in the development of balanced ethical decision-making processes is **systems thinking**, an approach that emphasizes the interconnectedness of components within a whole, suggesting that the overall behavior of a system results from these interactions. It promotes a holistic (synthetic) view rather than a fragmented (analytical) one, advocating that understanding the entire structure and its patterns is crucial. Systems thinking is based on general systems theory, which argues that all systems have components that are interrelated to create an organized whole. Systems thinking enhances ethical reasoning by emphasizing holistic analysis of the interconnected components and relationships within complex situations. This allows for a broader understanding of direct and indirect impacts.

In contrast, the **DIKW pyramid**, which is a hierarchy often used in information management and knowledge creation, represents an approach that focuses on the distinction between disparate elements (refer to Figure 12.2). Data, information, knowledge, and wisdom (DIKW) form the pyramid. Data at the pyramid's base signify raw, unprocessed facts and figures without context. Moving up the pyramid, data transform into information, where data are given context and meaning. Further refinement and understanding lead to knowledge, which is the application of information. At the apex, wisdom represents a deep, intuitive understanding or insight derived from a comprehensive synthesis of knowledge.

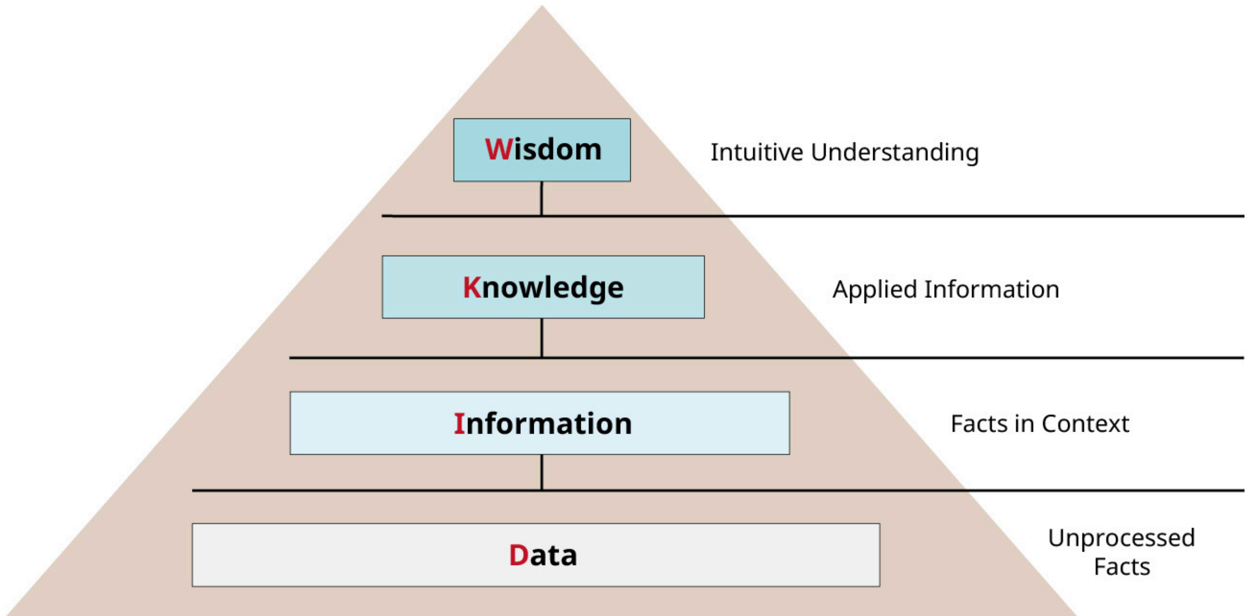


Figure 12.2 As the DIKW pyramid shows, data transform into information, which becomes knowledge, and ultimately wisdom. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

Application of the DIKW pyramid to systems thinking can provide guidance for decision-making. Data, in isolation, can be likened to individual components of a system. Without context or connection, these components (or data points) may seem unrelated or arbitrary. However, progressing up the DIKW pyramid, these isolated pieces start to form patterns (information), which when understood within a broader framework offer insights (knowledge). Finally, when these insights are synthesized in consideration of the whole system, holistic strategies (wisdom) emerge. Through systems thinking, the DIKW pyramid is not merely a linear progression from data to wisdom but a dynamic, interconnected web where each level informs and is informed by the others.

Ethical considerations are more present as you progress up the pyramid toward the wisdom level. At these higher levels, application of knowledge in business situations becomes more important, and ethics is required to make good decisions. In other words, as you move from the data level to the wisdom level, there are more opportunities for unethical decision-making.

In essence, systems thinking enhances the DIKW pyramid by emphasizing the importance of viewing each level as part of a larger, interconnected whole. It reminds us that wisdom is not just the culmination of accumulated knowledge but also the recognition of patterns, relationships, and feedback loops within the system. By understanding systems thinking, we can harness a deeper, more holistic understanding of complex issues and challenges, fostering more informed and effective ethical decision-making.

Sustainability and Information Systems

In the current technological era, information systems serve as the backbone of organizational operations. The integration of information systems into nearly every facet of business and daily life has created a modern world in which data flow is vital. Technology allows organizations the opportunity to move toward a more integrated and efficient future. But the evolution and expansion of these systems also have environmental, social, and economic impacts. Consequently, the **sustainability** of digital systems must be examined in the same way that society scrutinizes the sustainability of physical infrastructures. To manage this appropriately, ethical decision-making is vital.

Information systems and sustainability can determine an organization’s long-term viability and its broader impact on society and the environment. How can systems be designed and utilized that uphold the principles of long-term ecological and social responsibility and ensure that the digital tools are developed and maintained with a conscientious commitment to the well-being of the planet and its inhabitants?

Green, Lean, and Sustainable Information Systems

Information systems have become foundational to almost all business operations, and they have environmental and societal implications. To address these concerns, future information system professionals must become familiar with and understand three information system models: Green, Lean, and Sustainable. These models can be implemented with consideration of utilitarianism, deontology, and virtue ethics.

Representing a commitment to environmental stewardship, **Green IS** encompasses the strategies and practices designed to minimize the environmental footprint of digital operations. In this model, ethical choices are being made at all phases of the life cycle of information systems products. The practical implementation of the Green IS model's ideals means that the design, usage, disposal, and even recycling of information systems are environmentally friendly. The purpose of such practices is to reduce energy consumption during system operations, minimize greenhouse gas emissions, and carry out recycling and ethical disposal of electronic components. Given the growing demand for data centers and information technology infrastructure, the critical need for such practices will only increase in the future. Adopting environmentally conscious practices can offset these facilities' massive energy consumption and emissions.

Lean IS originates from embodying ideals in the manufacturing field; **Lean IS** is a set of practices that is about doing more with less, focusing on eliminating waste, in terms of time, resources, or processes, and thus ensuring that every aspect of an information system delivers value. Given the holistic nature of Lean IS, it involves efficient practices across a wide range of the information system life cycle. For example, within the context of process optimization, workflows would be streamlined to eliminate waste in the form of redundancies, and in resource management, both hardware and software would be utilized in a more efficient manner.

Continuous improvement can be accomplished by regularly assessing and refining system components for efficiency. One important task of Lean IS is to learn how a system works by analyzing its component parts and determining their relationships to one another. If done properly, such efforts will help managers better understand the underlying principles that lead to a better functioning system because they are better synthesized within the larger system. To accomplish this, leaders must understand the relationship between the information system and the organization. Then, they must expand that understanding to the local community where the organization is located. Beyond that lies the larger society within which that community is located and that society (be it at the state, federal, or international level) operates within the context of the planet Earth. All these systems are interrelated and impact each other in various ways. So, whatever information system you are working on, realizing the significance of your efforts does not end with performing your work-related task utilizing an information system. In keeping with Lean IS practices, the by-products of improving the efficiency of an information system include faster decision-making, reduced operational costs, and increased customer satisfaction.

While Green IS and Lean IS address environmental concerns and efficiency, respectively, **Sustainable IS** provides a more holistic approach that considers the long-term impacts and viability of information systems, focusing on their environmental, economic, and social implications. In fact, these can be understood as the three pillars of sustainability. From an environmental perspective, this approach mirrors the goals of Green IS, emphasizing reduced resource consumption and an environmentally conscious approach. The economic perspective focuses on the system's economic viability, ensuring that it delivers value. From the social perspective, the system should address social needs, foster inclusivity, and seek to reduce existing inequalities.

Sustainable IS can help organizations align the goals of a business with the larger systems that the business is a part of, thus creating opportunities for greater societal and environmental well-being. By-products of this alignment include enhanced corporate reputations, improved stakeholder relations, and long-term business resilience. Increasingly, corporate stakeholders are pressuring companies to have more sustainable practices.

As society grapples with rapid technological advancements, the integration of sustainability principles into information systems becomes paramount. Green, Lean, and Sustainable IS frameworks ensure that as technology progresses it is done responsibly. By embracing these principles, organizations can drive innovation as well as enhance the well-being of our planet and its inhabitants.

CAREERS IN IS

Sustainability Officer Roles

Sustainability officers help their organizations become more efficient and effective in ways that practice economic, environmental, and social responsibility. Corporate sustainability officers oversee company practices across dimensions like energy, waste, supply chain ethics, and social impact. Leveraging skills from various fields like systems analysis, project management, data analytics, and communication is crucial for this role as it involves guiding responsible operations.

Sustainable Consumption and Production

With information systems increasingly dominating both business and personal contexts, the ripple effects of our digital choices are becoming increasingly evident. The ethical dimension of these choices is highlighted when we consider the **sustainable consumption and production (SCP)** of information system resources, which focuses on using and producing goods and services in a way that minimizes environmental impacts while ensuring that resources are used efficiently. When information system resources meet SCP standards, they can meet the basic needs of the present without compromising the ability of future generations to meet their own needs.

The SCP approach not only addresses environmental and resource-related concerns but also delves into the moral responsibilities tied to technology creation and usage. The design, manufacture, use, and disposal of digital tools can either promote sustainability or exacerbate existing ecological and societal problems. Three areas where ethical issues emerge in this context are consumption, production, and policy regulation (Figure 12.3).

CONSUMPTION	PRODUCTION	POLICY
• Longevity • Repairability • Efficiency	• Sustainable design • Energy efficiency	• Federal, state, and local laws to support sustainable practices • Tax incentives and grants • Penalties for harm

Figure 12.3 Sustainability requires organizations to make sure their information systems meet consumption, production, and policy standards that benefit ecological and societal goals. (attribution: Copyright Rice University, OpenStax, under CC BY 4.0 license)

When considering the ethical consumption of information system resources, one key stakeholder is the consumer. It is essential to recognize that every digital device purchased or piece of software installed comes with an environmental and social cost. One's **ethical consumption** means being aware of this impact and making choices that prioritize longevity, repairability, and efficiency. With rapid technological advancements, devices become obsolete quickly, leading to substantial e-waste. Ethical consumption involves choosing devices designed for longer life spans and ensuring proper recycling or disposal of obsolete technology.

The production of information system products is also embedded with ethical considerations. Ethical production in information systems begins at the design phase. Embracing principles like modularity can make devices more repairable and upgradable, thereby extending their useful life and benefiting the larger system that comprises the information system and the planet as a whole. To benefit all stakeholders, the processes employed in producing digital tools should be energy efficient and minimize waste.

Governmental and international bodies create the legal framework for any particular information system, so policy and regulation play a role. Information systems are contained within the organizations that house and utilize them. These systems are utilized to interact with customers and other stakeholders that reside on our planet. Governmental and international bodies have a role in establishing standards that guide the ethical and sustainable production and consumption of information system resources. Beyond establishing laws, governments at the local, state, and federal level can encourage sustainable practices. Examples include tax incentives for using greener materials, grants for businesses that are more energy efficient, and credits to companies that reduce carbon emissions. Alternatively, these same entities can issue penalties and sanctions if laws are violated, thereby deterring environmentally harmful operations.

The nexus between ethics, sustainability, and information systems is evident in the realm of SCP, where all digital stakeholders—whether as consumers, developers, or policymakers—hold a collective responsibility. Adopting SCP principles within information systems ensures progress toward a digital future that is in harmony with the planet and its diverse inhabitants.

Sustainable Supply Chain Management

Supply chains are more than just logistic networks—they also represent a company's ethical principles, reflecting how its employees act within its organizational structure as well as the organization's natural obligation to practice societal and environmental responsibility in its actions. A **sustainable supply chain management (SSCM)** approach seeks to infuse sustainability principles into the supply chain process. The production of digital devices often involves complex global supply chains. Ensuring that materials are sourced responsibly and workers are treated fairly is vital. Ethical production prioritizes conflict-free minerals, promotes fair labor practices, and avoids environmental degradation. This is demonstrated, for example, in IKEA's commitment to using only recycled and renewable materials in their products.[3]

SSCM goes beyond optimizing traditional supply chain objectives, emphasizing instead the three Ps: people (social), planet (environmental), and profit (economic). This holistic approach ensures that businesses thrive for future generations. With their analytical and integrative capabilities, information systems are poised to play a pivotal role as the backbone of modern supply chains, providing real-time data, analytics, and communication tools. When utilized pursuant to SSCM principles, they can promote transparency, efficiency, and sustainability.

Sustainable sourcing is one component of the sustainable supply chain system that can be improved. A supplier evaluation platform is an information systems tool that can help accomplish this goal. This platform can automate the process of assessing suppliers based on their environmental and social practices and ensure that businesses partner with like-minded entities. Another practice related to sustainable sourcing is material traceability systems. These systems provide data about the origins of materials, allowing for responsible sourcing and avoiding the utilization of resources linked to environmental harm or unethical practices.

Another goal of SSCM is efficient and green logistics. One example of how information systems contribute to this practice can be seen through route optimization software. This software minimizes transportation costs and emissions by identifying the most efficient routes for the movement of goods. Similarly, inventory management systems can be utilized to optimize stock levels and reduce waste. The proper use of these systems ensures that resources are utilized judiciously, aligning with the tenets of SSCM.

One way an organization can demonstrate transparency is by using blockchain as part of its supply chain. Blockchain technology, with its decentralized and tamperproof nature, can trace products throughout their life

3 "Materials Are Key for Becoming Circular," IKEA, accessed December 23, 2024, https://www.ikea.com/global/en/our-business/sustainability/renewable-and-recycled-materials

cycles (refer to Chapter 10 Emerging Technologies and Frontiers of Information Systems). This fosters transparency and assures stakeholders of product authenticity and ethical sourcing. Another practice to enhance transparency is to incorporate effective stakeholder communication. Information system–enabled platforms facilitate open dialogues with stakeholders, updating them on supply chain practices and receiving feedback to continuously refine SSCM strategies.

The future for SSCM is continuous improvement and innovation. This will allow businesses to update their strategies and stay ahead of regulatory and market changes. Another SSCM development is collaborative ecosystems. Companies, suppliers, and tech providers, along with other pertinent stakeholders, should collaboratively explore innovative information system solutions that push the boundaries of current SSCM thinking to improve the supply chain process. Supported by robust information systems, SSCM offers businesses a pathway to reconcile operational efficiency with sustainability imperatives.

Corporate Social Responsibility

As businesses leverage technology at a rapid pace, the way they approach, integrate, and manage information systems can have lasting effects on societal welfare, environmental sustainability, and corporate integrity. Because the digital realm intersects with every facet of modern life, information systems plays an integral role in **corporate social responsibility (CSR)**, is an inherent recognition of the ethical relationship between a corporation and the larger social and environmental system that it inhabits. Corporate social responsibility allows companies to take responsibility for the impact their activities have on the environment, society, and stakeholders impacted by the company’s actions. It goes beyond focusing on profitability to consider the ethical implications of business operations. Information systems—which include tools, networks, and infrastructures—serve as both an operational backbone and a strategic asset for companies. The way businesses choose to deploy and manage information systems can either enhance or hinder their CSR goals.

When considering how to deploy and manage their information systems and technology, organizations need to take into account the three Ps of CSR:

- People represent the practices that will be followed as part of information system and technology operations.
- Planet represents consideration of the impact these operations will have on the environment.
- Profit is the economic goal that has to be sustained by the business.

Using the three Ps as a guide, organizations can minimize any negative effects of their information system and technology practices on the environment and society as a whole while still making a profit.

Corporate social responsibility can also fit into the context of the ethical theories you’ve learned about. From a utilitarian perspective, CSR consider the consequences of a company's actions and prioritizes the actions that generate the most good for the most number of people on the planet. An organization focused on deontology would seek out the principles that inform a more ideal version of society and seek to act in accordance with those principles. From a virtue ethicist perspective, an organization would attempt to embody the virtues that would best lead to the experience of a beautiful, true, good, and flourishing life, then interact with society from that state of being.

As with environmental practices, there are many opportunities for integrating CSR principles in information system development. From whatever philosophical perspective a company approaches it, integrating CSR into information systems means ensuring that the organization’s software and hardware development processes are in alignment with ethical guidelines. This includes ethical choices that will impact society, such as open-source software adoption, transparent data management, and safeguarding of user privacy. Design phase choice involves sustainable hardware. The selection of energy-efficient hardware, minimization of resource use, and the promotion of recyclable components further align the ideal aspects of CSR and information systems in tangible ways.

Information systems can also be utilized to facilitate CSR initiatives. Information systems can provide powerful tools that companies use to track, monitor, and report their CSR activities. Advanced analytics can aid in assessing environmental impact, employee welfare, and community engagement, allowing for more informed decision-making. The critical part, obviously, is that these tools be used with the intention that corporations seek to create a more ideal form of responsibility to society.

Another area in which information systems can benefit CSR efforts is stakeholder communication. Modern information systems enable transparent and continuous dialogue with stakeholders. Through digital platforms, companies can communicate their CSR initiatives, gather feedback, and foster a culture of accountability and inclusivity.

The futures of CSR and information systems are continuously evolving. Businesses must be proactive, anticipating shifts and aligning information systems and business strategies accordingly. This will require collaborative approaches that form partnerships between businesses, governments, and society so the positive impacts of CSR-focused information system initiatives can be more ideally implemented. As systems thinking informs us, all things are interconnected. Given this, to practice and foster ethical conduct, you should consider how the singular information system that is the focus of your work fits into and impacts the overall system. By centering CSR in information system decisions and operations, companies can advance their business objectives and champion a more sustainable, equitable, and ethical digital future.

Sustainable Development Goals

In 2015, the United Nations established **Sustainable Development Goals (SDGs)**, a set of seventeen interconnected objectives aimed at addressing global challenges and ensuring a more sustainable future for humanity (Figure 12.4). The SDGs provide a comprehensive framework, touching on areas like poverty, health, education, and climate change, with the aim of fostering prosperity while protecting the planet. As we strive to achieve these ambitious targets, the role of information systems becomes paramount because through digitization, automation, and analytics, information systems have the potential to accelerate our journey toward achieving these global ideals.

1 No poverty	2 Zero hunger	3 Good health and well-being	4 Quality education	5 Gender equality	6 Clean water and sanitation
7 Affordable and clean energy	8 Decent work and economic growth	9 Industry, innovation, and infrastructure	10 Reduced inequalities	11 Sustainable cities and communities	12 Responsible consumption and production
13 Climate action	14 Life below water	15 Life on land	16 Peace, justice, and strong institutions	17 Partnerships for the goals	**THE GLOBAL GOALS For sustainable development**

Figure 12.4 Information systems play an integral part in the United Nations' Sustainable Development Goals by connecting communities and resources. (credit: modification of work "The 17 Sustainable Development Goals of the UN" by United Nations: The Global Goals/Wikimedia Commons, CC0 1.0)

The ethical use of information systems for the common good empowers the achievement of SDGs. Consider these examples of how information systems can contribute to specific UN goals:

- Goal 3: Good Health and Well-Being: Advanced health information systems, telemedicine platforms, and health analytics tools can revolutionize health-care delivery, especially in remote and underserved regions of our planet.

- Goal 4: Quality Education: E-learning platforms, virtual classrooms, and digital educational resources offer new ways to bridge educational gaps and reach learners worldwide.
- Goal 9: Industry, Innovation, and Infrastructure: Information systems support industrial innovation by optimizing supply chains, enhancing manufacturing processes, and fostering global collaboration through digital platforms.
- Goal 13: Climate Action: Environmental monitoring systems, climate modeling software, and data analytics can provide insights into climate change patterns and inform mitigation strategies.

Achieving the SDGs requires public-private partnership and collaboration. Governments, private sectors, and nongovernmental organizations (NGOs) can create synergistic outcomes, far beyond what each of them can do individually. Information systems are the technology that can connect these organizations to drive impactful initiatives. Local knowledge and global expertise can be harnessed to cocreate information system solutions that are tailored to specific SDG challenges. Integrating technology with purpose, leveraging its capabilities, and navigating its challenges with foresight ensures that information systems can serve as a powerful tool in achieving the global promise of the SDGs.

GLOBAL CONNECTIONS

Sustainability Trends across Nations

Information system sustainability initiatives that attempt to address economic conditions, social values, and environmental priorities vary across the globe. For instance, the European Union has encouraged more robust e-waste recycling programs.[4] Samsung has introduced the Samsung Care for Clean India program to educate on e-waste disposal.[5] And Sweden's EcoDataCenter has switched from fossil fuel to hydrotreated vegetable oil to become a leader among Nordic countries in sustainable data centers.[6]

Creating flexible frameworks that are adaptable across nations facilitates global progress on shared imperatives like climate change. International bodies, such as the United Nations, promote sustainability best practices that can be customized. Grassroots community engagement also aids localization. Understanding national and cultural contexts enables stakeholders to create tailored road maps toward a common shared vision of responsible innovation.

Impact of Ethics and Sustainability on Information Systems and Information Technology

The development and utilization of information systems and technology have wide-ranging impacts on society, the environment, and the ethics of human-computer interaction (HCI). It is crucial that as these systems evolve, we remain cognizant of these impacts and align technological progress with ethical and sustainable ideals. Information systems intersect with ethics, social welfare, and ecological responsibility in several key areas.

Human-Computer Interaction

Human-computer interaction examines the interface between human beings and computing technology. As information systems become more sophisticated, with abilities like natural language processing, computer vision, and predictive analytics, new ethical considerations emerge regarding how these technologies are designed and deployed.

4 "E-Waste in the EU: Facts and Figures (Infographic)," Directorate General for Communication, European Parliament, March 21, 2024, https://www.europarl.europa.eu/pdfs/news/expert/2020/12/story/20201208STO93325/20201208STO93325_en.pdf
5 "About the Program," Samsung Electronics, accessed December 23, 2024, https://www.samsung.com/in/microsite/care-for-clean-india/?srsltid=AfmBOooC2fRGHen_hcSlMFEDCW07X6kepUHEY5vks0g7AGGhloWGeB53
6 "Sustainable Data Protection: EcoDataCenter in Sweden Relies on *mtu* Backup Generators from Rolls-Royce That Run on HVO Fuel," Rolls-Royce, November 14, 2024, https://www.rolls-royce.com/media/press-releases/2024/14-11-2024-sustainable-data-protection-ecodatacenter-in-sweden-relies-on-mtu-backup-generators.aspx

The key ethical issues in HCI involve transparency, privacy, and accountability. Systems should be transparent regarding their capabilities and limitations. Privacy must be safeguarded, and user data must be utilized ethically. Engineers must be accountable for potential harm resulting from flawed system design. Guidelines such as value-sensitive design promote these ideals by integrating ethical considerations into the design process. Overall, responsible HCI requires aligning systems with human values like trust, dignity, and justice.

ETHICS IN IS

Five Principles of Data Ethics

Collecting user data raises tensions between business interests and privacy rights. While mining data can optimize services, consent and transparency are essential. Harvard Business School identified five principles important for data ethics: ownership, transparency, privacy, intention, and outcomes.[7]

The ownership principle dictates that organizations cannot take individuals' data without their consent, and the transparency principle stresses the importance of informing individuals about how their data will be used. Privacy is important because even when individuals agree that their data can be used, their privacy must be respected. The intention principle cautions organizations to analyze why they need data to ensure that their intentions and reasons for collecting data are ethical. Finally, the outcomes principle notes that even with good intentions, data usage can lead to outcomes that harm individuals or groups, such as when data seem to show that certain groups are more likely to be associated with criminal activity.

User Experience

The user experience (UX) refers to how end users interact with information systems and their perceptions regarding accessibility, usability, and satisfaction. User experience design has ethical implications in terms of promoting inclusion and minimizing harm.

Inclusive UX design, such as video captioning, provides accessibility to groups with different abilities in hearing, vision, language or digital literacy. User experience should also seek to avoid **dark patterns**, deceptive interfaces that bait and switch to nudge users toward harmful actions, such as buying overpriced products. Misinformation, addictive behaviors, and compulsive spending can result from such exploitative designs. Responsible UX upholds ideals of autonomy and well-being by empowering users with controls, protections, and transparency.

Technology Adoption and Resistance

The adoption or rejection of new technologies has wide-ranging ethical and societal impacts. Some key societal considerations include the displacement of workers whose skills become obsolete, worsening inequality between technology adopters and nonadopters, and the environmental sustainability of proliferating hardware and infrastructure. Responsible innovation requires foresight and mitigation of these consequences. For example, change management processes can provide support and training to workers transitioning to new roles. Inclusive policies work to close digital divides by making technology affordable and accessible. Sustainable design and manufacturing should be pursued to lower the environmental harms of constantly evolving technologies.

7 Catherine Cote, "5 Principles of Data Ethics for Business," *Business Insights* (blog), Harvard Business School Online, March 16, 2021, https://online.hbs.edu/blog/post/data-ethics

Technology Addiction

Problematic overuse of technology and information systems can result in behaviors that negatively impact mental health and relationships (Figure 12.5). Psychologists point to dopamine-driven feedback loops that make devices habit forming.[8] For example, many apps have infinite scrolling that makes it hard for users to stop. Tech companies face ethical questions around deliberately engineering addictiveness into apps and platforms. Mitigating technology addiction requires design practices that promote healthy engagement aligned with user well-being. Examples include digital detox features, usage dashboards, and nudges toward positive habits. Families and schools also play a role in promoting tech-life balance and modeling healthy technology integration. Ongoing research and open dialogue around technology's addictive potential are warranted.

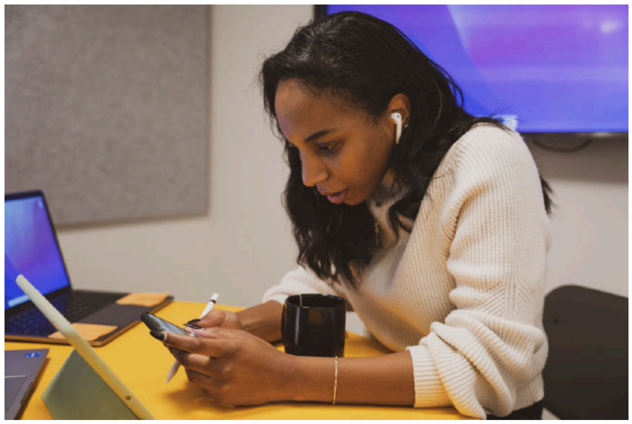


Figure 12.5 As we become more reliant on technology, this can lead to technology addiction, which occurs when we overuse technology and become so addicted to our cell phones and other technology that it negatively impacts our lives, including relationships with others. (credit: "Focused Female Professional at the Office" by Aspen/nappy, Public Domain)

Robotic and Artificial Intelligence Replacement of Humans

Advances in robotics and AI raise concerns about human jobs being lost to automation. This has significant ethical and social implications in terms of employment and economic security. However, robots and AI also create new roles, such as AI research scientists who study and create new AI technologies. Responsible AI specialists ensure that AI technology is managed ethically and legally for the company and society at large. Also, since robots and AI do not have some human skills such as creativity and empathy, humans are still needed to oversee tasks completed by robots and AI.

A balanced approach recognizes the benefits of emerging technologies while proactively addressing their disruptive effects. Policies like educational and training programs can help workforce transitions. Continual investment in human capabilities less prone to automation is needed, along with designing complementary roles between humans and AI. With foresight and intentionality, job displacement can ideally yield new potential.

Societal Implications of Technology

Some key societal implications stemming from the proliferation of information systems and technology include the following:

- Digital divide: The uneven distribution of access to information systems and information technology has created a digital divide between those who have access to technology and those who do not, reinforcing broader social and economic disparities. This has profound implications for education, employment, and social mobility. Individuals without technology access face constraints in pursuing educational opportunities, applying for jobs, using government services, and connecting with social groups. This

8 Anna Lembke, "Digital Addictions Are Drowning Us in Dopamine," *Wall Street Journal*, August 13, 2021, https://www.wsj.com/articles/digital-addictions-are-drowning-us-in-dopamine-11628861572

entrenches preexisting socioeconomic disadvantages. Policy steps like providing low-cost internet access, public technology centers, and digital literacy programs help bridge these divides. Inclusive design practices also ensure technologies accommodate users across age, ability, language, and socioeconomic status. Educational programs focused on digital literacy are also essential to ensure inclusivity. Pursuing digital inclusion promotes equity and social justice.

- Job displacement: The increased automation and use of information systems and information technology have led to job displacement in many industries, particularly in manual and routine-based roles. This has implications for the workforce, income inequality, and social welfare. Workers displaced by technology require retraining programs to transition into new roles. Policymakers must develop robust social safety nets to support workers struggling with job losses due to automation. Fostering a culture of lifelong learning and flexibility will be imperative as job disruption becomes more commonplace in our increasingly digital future.
- Cybercrime: The proliferation of information systems and information technology has also led to a rise in cybercrime, including identity theft, hacking, and online fraud. This has important implications for personal privacy, data protection, and security. Strict data privacy regulations and cybersecurity standards are required to safeguard users. Media literacy programs should educate the public on cyber risks. Cyber warfare also poses new national security threats that governments must address.
- Social media: The rise of social media platforms has significant implications for social interaction, communication, and identity. It has enabled new forms of social and political activism, both positive and negative. The platforms have been used to spread misinformation, exacerbate political polarization, and allow election interference. Features like social validation can be addictive and harmful. This is especially true for youth whose minds are more easily influenced given their stage of development. On the other hand, social media allows marginalized groups to build community and amplify their voices. Ongoing oversight, moderation, and user protections are needed to ensure social media minimizes detrimental impacts and instead works to benefit society.
- Health care: The use of information systems and information technology in health care has led to improved patient care, diagnosis, and treatment. However, it has also created new ethical and privacy concerns surrounding patient data and medical records. Strict data governance models, such as those found in HIPAA, must safeguard health-care data integrity and confidentiality. Careful oversight is required for emerging technologies, like AI diagnostics, to avoid harmful errors. Attention must also be paid to equitable access to health-care technologies.
- Environmental sustainability: The use of information systems and information technology can impact the environment in both helpful and harmful ways. Proliferating hardware and infrastructure contribute to resource consumption and e-waste. However, systems can also enable remote collaboration, thereby reducing transportation and associated emissions. Green design, renewable energy, and proper e-waste disposal are imperative for environmentally sound systems.
- Social and cultural impacts: Information systems and technology have influenced social norms, behaviors, and values both positively and negatively. For example, information systems and technology have been a positive force by helping people communicate over long distances to maintain close relationships, enabling people to learn about cultures worldwide without traveling. However, information systems and technology also provide resources to enable cyberbullying, allowing bullies to widen the circle of people they can harass. These examples indicate that ongoing research into how technology shapes social patterns is needed, along with thoughtful application of this knowledge to guide ethical and prosocial innovation.
- Privacy and data protection: Information systems' collection, use, and dissemination of personal data raises critical privacy issues. Data breaches, surveillance, and inadequate consent processes can violate user privacy. Strict data governance frameworks must safeguard personal data. Encryption, access controls, and principles like data minimization help protect privacy. Education on managing digital footprints is also essential.
- Cybersecurity and information security: Connected systems enable new forms of criminal activity,

including hacking, malware, and phishing. This can result in fraud, identity theft or disrupted critical infrastructure. To control cybercrime, implementing robust cybersecurity defenses via tools like firewalls and access controls is imperative. Workforce education on security best practices and law enforcement training to address cyber threats are needed. Information security must constantly evolve to stay ahead of criminal misuse of technology.

- Intellectual property rights: Emerging technologies like AI and social media raise new issues surrounding copyright, fair use, trademarks, and patents. Clearer legal guidelines are required. Ethical considerations around equitable access to knowledge must also guide intellectual property policies. Education on issues like plagiarism and piracy helps foster respect for IP rights.
- Ethical use of technology: The responsible use of information systems entails thoughtful practices regarding transparency, accuracy, bias mitigation, and fostering positive social outcomes. Corporate ethics policies guide issues like hacker ethics and responsible disclosure. Promoting public discourse on ethical technology, its management, and its use is key. The IEEE TechEthics is an extensive resource that addresses the ethical use of technology in business and society.[9]
- Ethical AI and automation: AI and automated systems raise concerns like privacy, embedded biases, and accountability. Ensuring human oversight and rigorously testing systems for fairness and safety are essential. Transparent and ethical AI practices consider potential harm early in the design phases. Regulations may be required to align automated technology with human values and welfare.

Responsible innovation considers the multifaceted societal impacts of information systems and technology. By upholding ethical principles and humanistic values, information systems can be shaped and governed to maximize society as a whole. Technology and society evolve together. Aligning the rapid pace of innovation with the public interest necessitates sustained dialogue between policymakers, technologists, and communities.

12.2 Intellectual Property

Learning Objectives

By the end of this section, you will be able to:

- Identify U.S. intellectual property laws and regulations
- Describe intellectual property in information systems and technology
- Describe the global initiatives to protect intellectual property

The culture and economy of the United States are becoming increasingly knowledge based, with a growing focus on technological innovations. In a 2022 report, the U.S. Patent and Trademark Office noted that intellectual property–intensive industries, such as computer technology and information systems, represent $7.8 trillion in economic value. This significant figure represents over 40 percent of the U.S. gross domestic product and accounts for forty-seven million jobs.[10] From an economic perspective, IP-related technology is significantly increasing.

Recall that intellectual property consists of creations of the mind like inventions, literary and artistic works, designs, symbols, names, and images used in commerce, protected by law from unauthorized use or replication. The area of law that concerns the realm of these creations—including technological creations—is known as **intellectual property law** and covers trademarks, trade secrets, patents, and copyrights. Such laws protect the creations of innovative labor, allowing the creators to benefit from their work. This incentivizes individuals and organizations to invest their time, energy, and resources into creating new technologies and systems. Intellectual property rights, when properly managed, have the potential to drive technological progress, fuel economic growth, and enhance societal welfare.

9 "Ethics Frameworks," IEEE TechEthics, accessed December 23, 2024, https://techethics.ieee.org/ethics-frameworks
10 Andrew A. Toole, Richard D. Miller, and Nicholas Rada, *Intellectual Property and the U.S. Economy*, 3rd ed., (U.S. Patent and Trademark Office, March 2022), 3–5, https://www.uspto.gov/sites/default/files/documents/uspto-ip-us-economy-third-edition.pdf

U.S. Intellectual Property Laws and Regulations

Intellectual property laws in the United States consist of four different areas of law: copyright law, patents, trade secrets, and trademarks, which are compared and contrasted in Table 12.1. These four areas are designed to incentivize the creation of various types of information and protect the owner from infringement by others.

	Copyright	Patent	Trade Secret	Trademark
Definition	An original work of authorship	Any manufacture, machine, process, or composition of matter that is considered new and useful	Information valued because not generally known, efforts to keep it secret	Any symbol, name, word, or device that distinguishes a good or service from those offered by competitors
Examples	Books, movies, fine art, architecture, software	Industrial machinery, biotechnology, manufacturing processes	Formulas, source code, prototypes, customer lists	Brand names, logos, trade dress
Requirements	New, useful, nonobvious	Originality and fixation	Information derives value from not being generally known, reasonable efforts to maintain secrecy	Use in commerce
Filing Required	No	Yes	No	No
Rights	To reproduce, distribute, or publicly perform/ display the work, and/or make derivative works	To make, use, sell, and import the patented invention	Efforts to prevent others from misappropriating the trade secret	Efforts to prevent uses of confusingly similar marks
Duration	Life of author plus seventy years	Generally, twenty years from the date of filing	Potentially indefinite	Potentially indefinite

Table 12.1 Intellectual Property Protection Summary Chart It is important for information systems professionals to understand intellectual property laws.

Copyright Law

The foundation for **copyright law** is found in the U.S. Constitution, which grants, in Article 1, Section 8, "Authors and Inventors the exclusive Right to their respective Writings and Discoveries" to "promote the Progress of Science and the useful Arts."[11] The Copyright Act of 1976 is the congressional statute that governs this form of IP.

The purpose of copyright law is to encourage the spread of knowledge by incentivizing authors to create new works. This is accomplished by granting the author of a work the exclusive right to reproduce, distribute, publicly perform or display the work, and also to make derivative works for a period of time that lasts for the life of the author plus seventy years. Examples of creations that can be copyrighted include books, architecture, musical works, movies, and—of particular interest to information systems professionals—software.

There are two requirements for an author seeking to obtain the protection of copyright law. The first is that the creation must be original, meaning it must be independently created and have some minimal degree of creativity. For example, simply alphabetically arranging a list of names and phone numbers will not meet this originality requirement. However, organizing that list by geographic areas would be enough to meet this minimal threshold. The second requirement is that the creation be fixed in a tangible medium of expression. This is so that it can be perceived or communicated to others. An example of this would be writing something down on a piece of paper. In the context of information systems, however, the creation is usually fixed in a computer file located on a hard drive.

Once an author creates a protected work and fixes it in a tangible medium of expression, it automatically gains copyright protection—meaning, no registration is required. However, registration of the work does provide certain benefits, including the ability to sue for copyright infringement in federal court.

Note that you cannot copyright an idea; only the *expression* of an idea merits legal protection with this form of IP. For example, suppose you came up with the idea and process for powering cars by saltwater instead of gasoline and proceeded to write a book about it. It would be legal for someone else to read that book, extract the idea and process for how to make cars run on saltwater, and build such a car, all without infringing your copyright. In addition to excluding protection for ideas (and instead protecting their expression, as in a book), copyright law does not cover a "procedure, process, system, method of operation, concept, principle, or discovery."[12] The protection of these would require a different form of IP, a patent.

The duration of a copyright is the author's life plus seventy years. This, plus the fact that copyright protection attaches automatically, leads to a great deal of information being protected for a long period of time. With the rise of the internet, a new movement arose to counter this: the **open-source** model, which means that content is open to everyone rather than being locked down via copyright. The emergence of open-source software has led to a great deal of collaboration and innovation, resulting in creations like Linux and open educational materials.

There is one significant aspect of copyright law that allows individuals to freely use copyrighted material: **fair use**, which is a principle that allows limited parts of works to be used for specific purposes like classroom activities, news reports, commentary, and criticism. To determine whether the use of copyrighted material falls within fair use, courts apply a four-factor test:[13]

- Purpose and character of the use (educational or commercial)
- Nature of the work (level of creative expression)
- Scope and substantiality (how much and what parts)

11 "Constitution of the United States: Article I, Section 8," *Constitution Annotated*, Congress.gov, https://constitution.congress.gov/constitution
12 "Ideas, Methods, or Systems," Circular 31, U.S. Copyright Office, https://www.copyright.gov/circs/circ31.pdf
13 "U.S. Copyright Office Fair Use Index," U.S. Copyright Office, last updated November 2023, https://www.copyright.gov/fair-use/index.html

- Effect on the marketplace (negative impact on current market)

Of these factors, the effect on the marketplace is the most important. For example, if a professor were to use a five-minute clip from the movie *The Matrix* to teach the class about fight choreography, a court would most likely find that this was within fair use. This is because (1) the purpose and character of the use were educational in nature; (2) the substantiality of what was copied is only five minutes from a movie that was over two hours long, and most importantly; (3) the effect on the marketplace was negligible. In other words, the movie would not lose sales due to this act. In fact, some students might be interested enough in what they saw to view the movie, thereby increasing the revenue for the copyright holder. It should be noted that courts often weigh these factors differently depending on the specific case.

FUTURE TECHNOLOGY

Artificial Intelligence and Copyright Law

Advances in AI are generating new questions about how copyright law applies to content created or used by AI. This is especially true of generative AI computer programs such as ChatGPT, DALL·E 2, Stable Diffusion, and Midjourney. These programs can generate new output (images, text, and other content) after receiving input via a user's textual prompts. This is possible because they are trained on large quantities of existing works, much of which is subject to copyright protection.

Generative AI programs raise several novel legal issues under copyright law. For example, do the outputs of AI merit copyright protection? And if so, who is the owner of the copyrighted work? Does copyright infringement happen in an AI training process as it utilizes a large amount of copyrighted work to enable the AI to generate outputs? Do the outputs generated by AI infringe on existing copyrights? These questions and others are at the core of many legal battles and will continue to be addressed as AI technology evolves.

Patent Law

Also established by the U.S. Constitution, **patent law** protects any "new, useful, and nonobvious"[14] process, machine, manufacture, or composition of nature. To obtain patent protection, the inventor must file with the U.S. Patent and Trademark Office (USPTO) (Figure 12.6). After filing, the inventor can prevent others from making, using, selling, and importing the patented invention. Theoretically, this enables the inventor to recover the costs associated with developing the invention and to profit from its sale. Some examples of famous patents granted by the USPTO include Alexander Graham Bell's telephone patent, Thomas Edison's patent for the incandescent light bulb, and more recently, Jaap Haartsen's patent for Bluetooth communications.

14 U.S. Patent and Trademark Office, "General Information Concerning Patents," U.S. Department of Commerce, 2014, https://www.uspto.gov/sites/default/files/inventors/edu-inf/BasicPatentGuide.pdf

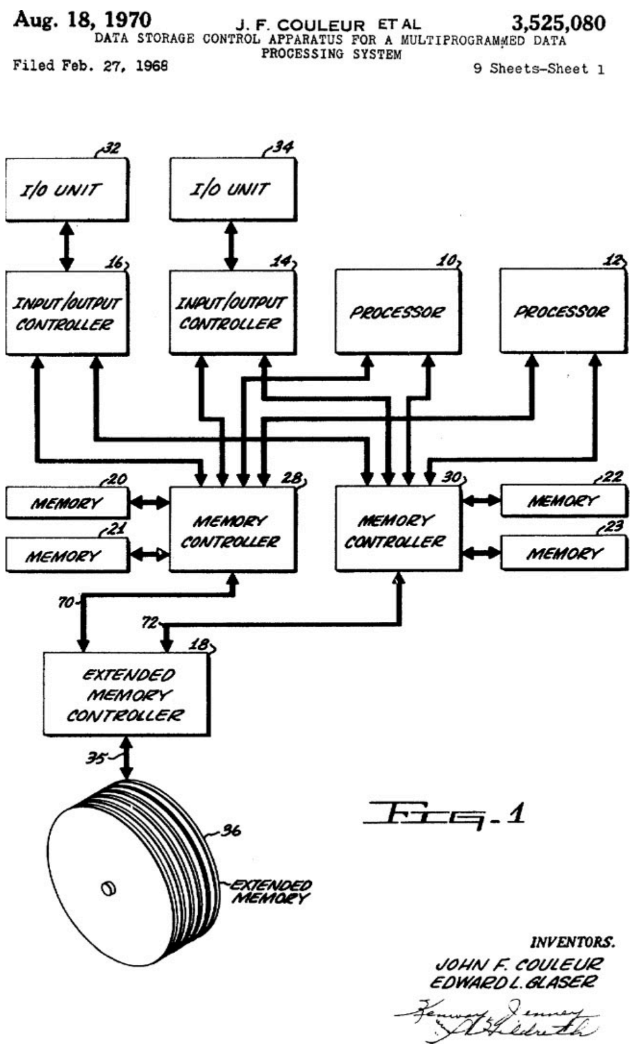


Figure 12.6 This is a 1968 patent for a "data storage control apparatus for a multiprogrammed processing system" developed by colleagues at MIT/General Electric. This diagram is of a mainframe, showing how it is connected to a memory unit. The numbers represent the part or component of the product. (credit: modification of work "US Patent connected to Project MAC (Multics project)" by Couler, Glaser, U.S. Patent Office/Wikimedia Commons, Public Domain)

Obtaining a patent is not a simple process as there are several requirements involved in gaining patent protection. First, a patent application is filed with the USPTO submitting a detailed description of the invention. The USPTO will then go through the intensive process of determining whether the submission merits patent protection. This process is complex and almost always requires the assistance of a patent attorney or agent. This cost combined with those associated with the research and development necessary to create a patentable invention result in the fact that most patents are quite expensive to obtain.

Once obtained, patents provide one of the strongest forms of IP protection. Any entity that uses the invention in any way is subject to patent infringement. Generally, the only way to use the patented idea is to pay the owner a fee to obtain a license. Additionally, it is not legal for anyone else to independently discover and use the invention. Furthermore, no one can reverse engineer the patented invention to determine the nature of the idea. Due to these powerful protections, the primary way a competitor would seek to utilize a patented invention without the creator's permission is by challenging the validity of the patent granted by the USPTO. As with obtaining a patent, the cost of litigation to challenge this form of IP is usually both very expensive and time-consuming.

CAREERS IN IS

Patent Agent and IP Lawyer Pathways

Aspiring patent agents and IP lawyers should pursue STEM (science, technology, engineering, and mathematics) undergraduate degrees, followed by law school and the patent bar exam. Gaining IP experience via legal clinics, USPTO programs, or law firm internships is advisable. Understanding technology and law provides a foundation for this complex specialty.

Trade Secret Law

The source of **trade secret law** resides in the Uniform Trade Secrets Act, which defines a trade secret generally as information that derives economic value from not being generally known and that efforts to maintain its secrecy are reasonable.[15] As you can imagine, various types of information can be protected, including business, financial, economic, technical, and engineering information. Specifically, formulas, patterns, compilations, programs, devices, methods, techniques, and processes can be subject to trade secret protection. The trade secret owner must ensure that the secrecy of the trade secret is maintained. Examples of such actions include nondisclosure agreements (NDAs), employee training, access controls, exit interviews, marking documents as confidential, IT security measures (such as firewalls and intrusion detection systems), and physical security measures (such as restricting access, security personnel, and CCTV monitoring). If the trade secret owner continuously maintains reasonable measures such as these, the duration of protection against misappropriation is potentially indefinite.

Trade secret protection can, however, be lost in several ways. First, competitors can legally reverse engineer any information that an organization maintains as a trade secret. Second, a competitor could independently discover the information that is being maintained as a trade secret, and the owner would have no cause for action. Finally, a competitor can lawfully acquire the information being protected. This can occur if the trade secret owner fails to take reasonable measures to maintain its secrecy. For example, posting a trade secret on a publicly accessible website will allow the competitor to lawfully acquire the trade secret. While these concerns are significant, companies often choose this form of protection over a patent because trade secrets can have a potentially indefinite term if properly protected, while a patent terminates after twenty years.

ETHICS IN IS

IP Laws and Access to Knowledge

While incentivizing innovation, IP laws can also restrict access to knowledge. Copyright terms that extend beyond an author’s life may impede public domain sharing. Due to stringent patent rules, patients can be denied access to affordable generic drugs. Creativity may be stifled if individuals are unable to access protected IP to develop ideas. To counter this and promote the free exchange of knowledge, IP regulations try balancing incentives and access but often favor proprietary interests.

15 “Trade Secret,” Legal Information Institute, Cornell Law School, last updated June 2024, https://www.law.cornell.edu/wex/trade_secret

Trademark Law

The foundational source of **trademark law** is the commerce clause of the U.S. Constitution, which allows Congress to regulate interstate and foreign commerce. The Lanham Act of 1946 is the statute that governs this area of IP law. Trademark law protects a “word, name, symbol, or design” used to identify the source of a good and distinguish it from the products of another.[16] Trademarks can be applied to product elements that make it uniquely identifiable in a market, such as specific shapes (like Coca-Cola’s bottle design), scent, colors, or packaging. Like copyright law, one does not need to register to receive trademark protection; however, doing so does provide certain benefits.

Trademarks are an essential part of almost any business. They provide consumers with a simple way to identify the source of a good or service, and are thereby crucial in building customer trust, brand recognition, and consumer loyalty. The duration of a trademark is potentially indefinite, though it can be lost for several reasons. For example, abandonment of the mark, which occurs when a trademark owner does not use the trademark for at least three years, will result in the loss of protection.

Ethical Issues in Intellectual Property Law

Intellectual property protections provide numerous benefits to individuals and organizations, but there are also significant ethical considerations associated with IP law. Intellectual property laws, especially copyrights and patents, incentivize creators to generate new information by providing them protection of that information for a period of time. However, the ultimate purpose of IP laws is to benefit society at large by providing its members access to new creations. This results in a tension between the rights of the creator and the rights of society. While the promotion of creativity and innovation is a worthy goal, IP laws also have the potential to restrict access to information and technology. This can potentially lead to digital divide issues, whereby certain specific individuals or communities are disadvantaged due to their lack of access to the new technology. Thus, governments and legal systems must strike an appropriate balance between incentivizing innovation and ensuring equitable access to new technology on a global scale.

Intellectual Property in Information Systems and Information Technology

Intellectual property laws play a significant role in information systems and information technology. These laws foster innovation and economic growth within the technology sector, but they come with a host of ethical considerations that must be managed appropriately.

Copyright Law in Information Systems and Information Technology

Copyrights are critical in protecting software, databases, and website content. Adobe Systems (Adobe) uses copyright law to protect its suite of creative software tools, including Photoshop, Illustrator, and InDesign. This protection extends to both the source code and the object code. Adobe has taken significant steps to combat software piracy, including filing lawsuits against individuals and organizations accused of infringing on its copyright. The company has established the Adobe Trust Center to proactively deal with fraud prevention. Their software offers automatic licensing checks through the Adobe Genuine Software Integrity Service. Copyright infringement can involve distributing or using unlicensed copies of Adobe’s software or cracking the software to bypass licensing protections. These measures taken are particularly important as pirated software undermines the financial stability of companies, like Adobe, that rely on the sale of licenses for their products.

Tech companies maintain websites to promote their business to clients. Amazon protects its product descriptions, promotional content, images, blog posts, and other Amazon-written material by copyright. This protection is aimed at preventing someone from legally copying the information contained therein and fixing it in another tangible medium of expression. It is also a violation of copyright law to scrape (that is, use automated tools, as you learned in Chapter 8 Data Analytics and Modeling, to extract data) Amazon’s site

16 U. S. Patent and Trademark Office, “U. S. Trademark Law: Federal Statutes,” November 25, 2013, 41, https://www.uspto.gov/sites/default/files/trademarks/law/Trademark_Statutes.pdf

content without permission.

Copyright law also applies to databases, a critical component of information systems. Microsoft, for example, uses copyright law to protect its SQL server, a relational database management system. Both the source and object code used to create this database are protected by copyright law. While Microsoft's copyright covers the database, the copyright does not extend to data that users and organizations enter into the database: the data held within the database are the property of the user or organization that maintains it.

Sometimes the relationship between copyrights and patents can confusing. For example, software code may be protected by a copyright, while a unique user interface or algorithm may be protected by a patent. By using patents and copyright laws to protect their IP, Adobe, Amazon, and Microsoft are motivating their customers and competitors to use their products in an ethical and legal manner. In general, copyright laws promote ethical behavior throughout society by discouraging various unethical and illegal activities. For example, because of copyright laws, moviegoers are unlikely to sit in a theater and record a movie, authors are discouraged from plagiarizing another writer's work, and photographs are less likely to be used without permission.

Patent Law in Information Systems and Information Technology

As with copyrights, patents provide an incentive for organizations using information systems to invest in research and development. Patent law encourages innovation through this, and it also motivates ethical behavior regarding patents. One highly effective patent in the digital domain is Amazon's "1-Click" patent.[17] This innovation allows consumers to make purchases with a single click, significantly streamlining the online shopping experience. Although this patent expired in 2017, it gave Amazon a significant advantage in the e-commerce domain for many years, increasing market share and playing an important role in the online retailer's massive growth.

Blockchain is another example of a technological innovation that utilizes patent law for protection. IBM, one of the leading patent holders in the United States, has obtained numerous patents related to blockchain.[18] These patents give IBM twenty years of IP protection, enabling it to prevent others from utilizing its innovations. This helps guarantee more market share for IBM and can provide revenue streams if the company decides to license this technology to others.

Qualcomm is another tech company that utilizes patent protection for its innovations as part of its business model. As a market leader in wireless communications technology, Qualcomm holds over 160,000 approved and pending patents related to 5G technology.[19] These patents cover many components of 5G networks, including chips in devices and infrastructure equipment. Qualcomm has been able to leverage its research and development successes by entering into over 200 licensing agreements with other entities to use its protected technology. IP protection is a central component of the enterprise's goals of sharing its innovations while receiving fair value compensation.

Trade Secret Law in Information Systems and Information Technology

Trade secrets are critical to a tech company's business strategy. Complex algorithms are the most important asset in many tech company portfolios. Google's search algorithm, PageRank, which determines the ranking of web pages in a search result, is maintained as a trade secret. It provides a competitive advantage to Google and determines the access and visibility of online information.

Computer source code is another asset that many companies maintain as a trade secret. Oracle's database

17 R. Polk Wagner and Thomas Jeitschko, "Why Amazon's '1-Click' Ordering Was a Game Changer," Knowledge at Wharton podcast, September 14, 2017, 26 min. https://knowledge.wharton.upenn.edu/podcast/knowledge-at-wharton-podcast/amazons-1-click-goes-off-patent/

18 Kristopher B. Kastens and Timothy Layden, "Top Holders of Blockchain Patents," Kramer Levin, July 21, 2022, https://www.kramerlevin.com/en/perspectives-search/top-holders-of-blockchain-patents.html

19 "Qualcomm Licensing Drives Our Intelligently Connected World Forward," Qualcomm, accessed January 13, 2025, https://www.qualcomm.com/licensing

software is a major asset for the company. This proprietary information is protected as a trade secret, ensuring that the details of how the software works at the source code level are kept confidential. To keep this protection, the company takes numerous measures to maintain its secrecy.

A company's data collection, storage, and analysis methods involving big data are also considered trade secrets. Companies like Google use trade secrets to secure their customer data. These detailed data contain search histories, preferences, and passwords. Google uses this information to inform its search algorithm. In its YouTube platform, Google gives video recommendations, custom search results, and targeted ads based on users' searches, videos they watch, and how they interact with the website.

Trademark Law in Information Systems and Information Technology

Trademarks help companies brand themselves in the marketplace and are very valuable in the tech sector. Trademarks are often recognized as part of a company's intangible assets that give them a competitive advantage in the marketplace. One of the most iconic branding images is Apple's bitten apple logo (Figure 12.7). It is recognizable worldwide, identifies the source of the good, and distinguishes it from the products of another. Consumers who recognize this symbol on a product know they are purchasing from Apple.

(a) (b) (c)

Figure 12.7 Apple's bitten apple logo has been in use for 50 years. It identifies products created by Apple, such as (a) printers, (b) iPads, and (c) MacBooks, and assures consumers that they are purchasing genuine Apple products. (credit a: modification of work "Former Apple Logo" by "Cbmeeks"/Wikimedia Commons, Public Domain; credit b: modification of work "Apple tablet" by Carol Clarkson/Flickr, CC BY 4.0; credit c: modification of work "Apple Logo on MacBook" by Image Catalog, Unsplash/Flickr, CC0 1.0)

Another form of trademark protection is **trade dress**, which refers to the visual appearance of a product or its packaging. Google's minimalist search page design has this form of IP protection. Figure 12.8 shows the simple, clean design that ensures users they are indeed performing a web search on Google and not one of its competitors.

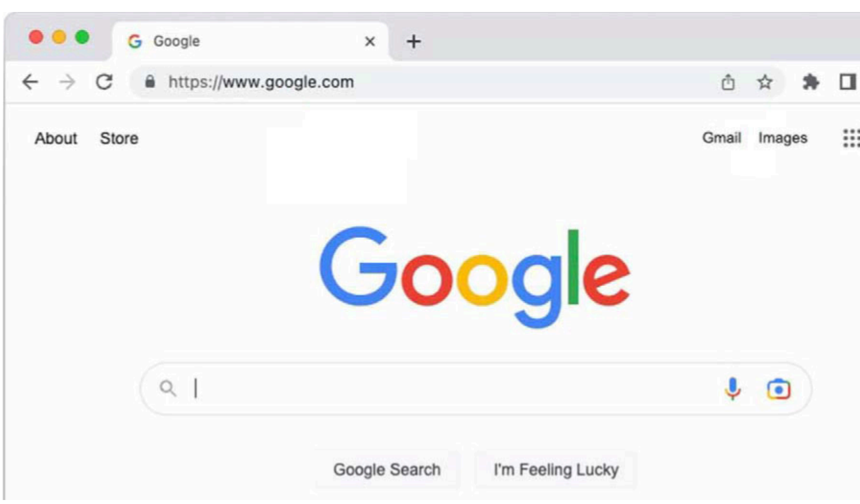


Figure 12.8 Google's minimalist search page design is an example of trade dress, and it is protected as intellectual property through trademark law. (credit: modification of work from *Workplace Software and Skills*. Google Search is a trademark of Google LLC.)

LINK TO LEARNING

The mission of the Center for Humane Technology is to align technology with the best interests of humanity—that is, the benefit of humanity and the planet as opposed to the financial interests of technology owners, especially in the design phase. To help meet that goal, the center has created a series of free interactive learning modules (https://openstax.org/r/109HumaneTech) for a Foundations of Humane Technology course. Check out the first module, called "Setting the Stage."

Global Initiatives to Protect Intellectual Property

The IP laws of the United States only represent one legal system of nearly 200 countries in the world. Consequently, several global initiatives attempt to synthesize the various IP laws of many countries. Two significant initiatives include the World Intellectual Property Organization (WIPO) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Because local laws differ across the world, professionals working internationally should become familiar with the laws where the company does business, and international laws are valid in a majority of the countries around the world.

World Intellectual Property Organization

The **World Intellectual Property Organization (WIPO)** is an agency of the United Nations created in 1967, with the mission to "lead the development of a balanced and effective international IP system that enables innovation and creativity for the benefit of all."[20] The WIPO serves a vital role in the information systems context, assisting in the synthesis of global laws governing system design, algorithms, and brand identities.

The WIPO seeks to harmonize international cooperation to create a legal framework that supports IP rights. To accomplish this, it administers dozens of international treaties that provide for the recognition and enforcement of IP rights. This assists those organizations that operate information systems on a global scale by providing protection in various jurisdictions for their creative output. The WIPO also provides services for trademark registration and an international patent system for patent applications.

Beyond these legal protections, WIPO seeks to create a more balanced and accessible IP system that offers benefits accessible to all countries. It does so by providing resources, education, and support for understanding IP rights. Additional initiatives include policy advice, legal and technical assistance, and capacity-building programs for developing countries. These efforts help emerging markets build a foundation conducive to technological innovation and creativity, thereby addressing ethical issues related to the digital divide.

Trans-Pacific Partnership

The **Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)** is an agreement among several Pacific Rim nations that, among other purposes, serves to set standards for intellectual property within trade agreements. It was created as an alternative to the Trans-Pacific Partnership Agreement (TPPA) after the U.S.'s withdrawal prevented its ratification. Countries participating in the agreement include Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the United Kingdom, and Vietnam.

The primary purpose of the CPTPP is to harmonize IP laws across the member nations. This involves setting common standards for copyright terms, patent protections, and trademark regulations. Having common standards allows businesses operating in a number of these countries to simplify their IP management. The agreement also extended the term of copyright protection to what is standard in the United States and Europe—that is, the life of the author plus seventy years. Trademark protection was also strengthened by

20 "WIPO," JPO Service Center, United Nations Development Programme (UNDP), accessed January 13, 2025, https://www.undp.org/jposc/wipo

expanding the definition of what qualifies as a trademark. Importantly, the CPTPP also establishes a system for registration and protection of geographic marks, which are trademarks that include a geographic location. Finally, the agreement establishes a strong legal framework for enforcement of IP rights. This includes civil and criminal penalties for IP violations.

Case Study: Intellectual Property

Your cousin, Priya, is a fellow information systems student and has come up with a new tool for IS data analytics. She has read all of the literature on the subject, and her professor, who is an expert in the field, has never seen or heard of anything like the tool she is proposing. Priya has been working on the design of this new tool throughout her undergraduate career, and as graduation approaches, she is eager to acquire the legal protections needed to properly protect her creation and introduce it to the world. In addition to the new tool, she has also come up with a name for the tool, “Ideal IS,” and wants to use these words to market the product. Additionally, Priya has written a 300-page book titled, *Ideal IS: The Future IS Now*. Finally, she has collected a curated list of over 60 professors, professionals, and friends who have told her over the years that they are interested in purchasing the new tool. Priya would like your help determining what steps need to be taken to protect her idea before its launch. Using what you have learned, and referring to Table 12.1, advise your cousin on the following questions:

- How should Priya protect her idea for a new IS data analytics tool? Should it be protected by a copyright, patent, trade secret, or trademark?
- How should Priya protect her book, *Ideal IS: The Future IS Now*? Recall that the book is different from the tool itself and will require different protection.
- How can Priya protect the potential customers list that she has curated over the years? Customer lists are not original works or designs that you created, but they still meet the criteria to be protected by IP laws. Explain how this can happen.
- How should Priya protect the words she wants to use to name and market the product, Ideal IS? Why? Remember that the words that name your product distinguish it from your competitors’ products, and IP laws protect this name.

12.3 Ethics of Artificial Intelligence Development and Machine Learning

Learning Objectives

By the end of this section, you will be able to:

- Describe the purpose of ethical governance and regulations for developing and using AI and machine learning products
- Discuss the impact machines using AI have on fairness, bias, transparency, and explainability

Artificial intelligence (AI) is a broad field that resembles human intelligence, including collecting information, understanding concepts, applying information, and making decisions. Machine learning is a subset of AI and refers to a specific technique that allows computers to learn from data. The ongoing development and growth of artificial intelligence and machine learning mean that leaders in the field must be guided by ethical principles and appropriate governance frameworks. Given the potentially significant impacts these technologies can have on society, individuals, and the environment, a comprehensive approach is needed to ensure they are harnessed responsibly. This includes **multistakeholder collaboration** that involves leaders of nations and organizations worldwide working together to address considerations around governance, fairness, bias, transparency, and explainability.

LINK TO LEARNING

Artificial intelligence offers exciting opportunities to improve our lives as it becomes interwoven into medical therapies, smart home devices, and strategic decision-making processes; however, AI presents challenges of balancing its capabilities with the need for good governance and ethical management. Learn more by exploring UNESCO's Recommendation on the Ethics of Artificial Intelligence (https://openstax.org/r/109EthicsofAI) and how its core values are being implemented by member states.

Ethical Governance and Regulations in Artificial Intelligence Systems and Products

The development and use of AI systems must be guided by clear accountability and responsibility frameworks to be ethical. Developers, deployers, and users of AI should be accountable for any adverse impacts resulting from flawed system design, limitations, or misuse, such as phishing or identity theft. Responsibility should be allocated across the AI value chain, from initial data collection and algorithm design to ongoing monitoring and maintenance. Legal regulations and industry standards help clarify where liability lies if harm does occur. For high-risk applications like self-driving cars or AI diagnostics, insurance may be warranted.

Another central ethical concern is protecting privacy and ensuring AI is secure from misuse or cyberattacks. As AI systems collect and analyze expansive datasets, robust data governance practices must safeguard personal information and prevent unauthorized access. Approaches to help mitigate private risks can include data minimization to limit data collection to information that is relevant and necessary, encryption to transform data into code, and access controls to regulate who has access to data. Ongoing security assessments of AI systems (review 5.1 The Importance of Network Security) will identify potential vulnerabilities to be addressed. Any data breaches or system compromises must be reported per breach notification laws.

To achieve these goals, maintaining meaningful **human control** and oversight over AI is critical. Humans—not fully autonomous systems—must remain ultimately responsible for high-stakes decisions. Artificial intelligence transparency, the ability to show that the outputs make sense, and results validation support human oversight. Humans may need to remain "in the loop" and check results when AI systems operate in real-time for critical use cases. Predefined constraints can also curb unfettered AI autonomy if human supervision is absent. The goal should be complementing human capabilities with AI, rather than replacing human discretion and authority.

In addition to oversight, AI systems must be transparent regarding their capabilities and limitations. Documentation, logging, and monitoring should provide visibility into system functionality. User interfaces should clearly convey when users are interacting with AI instead of a human being since this can be difficult to discern. Such transparency ensures appropriate trust in AI systems by aligning user expectations with actual performance. It also facilitates auditing algorithms for issues like bias or inaccuracies. Guidelines and frameworks have been introduced to provide standards for developing and managing autonomous systems. Examples are the IEEE Global Initiative for Ethical Considerations in AI and Autonomous Systems and the EU's European Commission's standards presented in their Ethics Guidelines for Trustworthy AI.[21]

ETHICS IN IS

Ethical Use of Chatbots

Chatbots interact with users in increasingly humanlike ways. This raises ethical concerns, especially if the chatbots are not designed transparently. For example, chatbots may be used to gather individuals' personal information, possibly violating their privacy. Chatbots can be manipulative, persuading users to make

21 "The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems," IEEE Standards Association, accessed January 13, 2025, https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/; "Ethics Guidelines for Trustworthy AI," European Commission, last updated January 31, 2024, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

unwise decisions or purchases. Chatbots can also be biased, which may negatively impact how they interact with humans.

To help ensure that chatbots are used ethically, chatbots should identify themselves up front as AI, and not pretend to be human. They also should provide options to opt out, including the option of dealing with a human rather than a chatbot.

Another key governance issue is ensuring that AI systems are free from biases. Training data and algorithms must be continually vetted to avoid encoding social biases and prejudices into systems. Diversity among AI development teams also helps reduce bias. Regular algorithm audits and bias testing identify problems that must be addressed.

To understand how a lack of AI accountability can cause harm, consider predictive policing algorithms. These algorithms have included biases that disproportionately target minorities. One example is PredPol, a predictive policing software tool used by the Los Angeles Police Department. With inadequate human oversight of the data and methods used by its algorithms, the flawed logic of the tool took a while to uncover. Eventually, its built-in loops and inability to reduce crime led to the department terminating its use. Related criticism has led to rebranding by PredPol (now Geolitica) and similar policing tools to focus less on predicting criminal events and more on improving policing transparency and accountability.[22]

Alongside algorithmic bias, safety is another ethical imperative for AI and machine learning. Even if unintended, errors or limitations in complex AI systems carry risks of harm. Rigorous testing protocols are essential, especially for physical systems like autonomous vehicles or medical robots. Simulation environments allow for safe evaluation of hazardous scenarios. Fail-safes and human oversight provide additional protection and backup. Organizations that adopt an open, proactive approach toward safety will engender greater public trust.

Sustainability is another emerging area of focus in AI ethics. The exponential growth of AI workloads has significant environmental impacts from energy consumption to electronic waste. Approaches like energy-efficient model design, low-emission chipsets, and carbon offsetting help mitigate this.[23] Artificial intelligence can also be explicitly leveraged for sustainability initiatives, such as mapping deforestation, making waste management more efficient, and predicting both weather events and climate disasters to help communities.[24]

Effective governance requires translating ethical principles into action via organizational policies, legal regulations, and industry norms. Governments must develop laws and policies tailored to the ethical use of emerging technologies, balancing innovation and responsible oversight. Companies should enact internal controls aligning AI development and usage with ethics and human values. They must also comply with evolving regulations. Global coordination will become more critical to synthesize governance across jurisdictions.

Finally, civil society plays a crucial role in advocating for ethical AI. Organizations focused on digital rights, consumer protection, and social justice can help manifest public concern. They can also advise institutions on how to translate idealistic AI principles into concrete daily practices. Ongoing stakeholder dialogue and public engagement will ensure governance keeps pace with technological change.

Realizing the benefits of AI while mitigating risks necessitates holistic governance that integrates ethics

22 Johana Bhuiyan, "LAPD Ended Predictive Policing Programs Amid Public Outcry. A New Effort Shares Many of Their Flaws," *The Guardian*, November 8, 2021, https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform
23 Paul Henderson, Jieru Hu, Joshua Romanoff, Emma Brunskill, Dan Jurafsky, Joelle Pineau, "Towards the Systematic Reporting of the Energy and Carbon Footprints of Machine Learning," *Journal of Machine Learning Research*, 21, no. 248 (2020): 1–43, https://www.jmlr.org/papers/volume21/20-312/20-312.pdf
24 Victoria Masterson, "9 Ways AI Is Helping Tackle Climate Change," World Economic Forum, February 12, 2024, www.weforum.org/stories/2024/02/ai-combat-climate-change/

throughout the technology life cycle. This requires foresight, responsibility, and coordination between stakeholders. If done comprehensively and with proper intention, AI can flourish in step with the enduring values of privacy, justice, autonomy, and human dignity.

Artificial Intelligence's Impact on Fairness, Bias, Transparency, and Explainability

As AI systems grow increasingly powerful and ubiquitous, ensuring they align with principles of fairness, accountability, and transparency becomes imperative. Without proactive efforts, AI risks perpetuating harm by amplifying historical prejudices, concealing decision logic, and displacing human oversight.

One major area of concern is that AI systems may discriminate against certain groups of people based on gender, race, age, or other attributes. If the data used to train algorithms contain social biases, such as information that promotes gender or racial stereotypes, AI can further engrain discrimination. Ongoing testing using diverse datasets is essential to uncover hidden biases. A **human-in-the-loop system**, which involves human contributions and feedback, also allows monitoring outputs for evidence of unfairness. Other best practices include data anonymization, **adversarial debiasing** to ensure AI is not biased by training examples, and **minority oversampling** to ensure balanced classes and sample sizes help mitigate prejudice.[25] Promoting diversity among AI development teams further helps uncover issues that need attention. Overall, reducing algorithmic bias is an ethical imperative for organizations deploying AI.

The need for transparency in how AI systems operate and make decisions is closely related. "Black box" models like neural networks can render decision logic opaque. However, documentation, logging, monitoring, and auditing capabilities can shed light on system functionality. User interfaces should clearly indicate when users interact with AI rather than humans. Such transparency fosters trust in AI's actual capabilities. Openly conveying system limitations also reduces the risk of overreliance or misuse. Across all contexts, transparency principles foster ethical use of AI.

Similarly, **explainability**—being able to convey the rationale behind AI decisions clearly—is crucial. While certain techniques like linear models or decision trees have self-evident logic, complex neural networks can be inscrutable. To properly question, validate, and enhance AI, developers should incorporate explainability capabilities into the development process wherever feasible. This might involve using localized interpretation methods or approximating models with more easily understood ones. While full explainability may not always be possible, aiming for intelligibility in design still promotes accountability.

LINK TO LEARNING

Explainability and [explainable artificial intelligence (XAI) development (https://openstax.org/r/109XAI)](https://openstax.org/r/109XAI) can be a valuable tool to help companies manage legal and ethical issues associated with AI. Explaining AI helps users understand the "why" and "how" aspects of AI, making them more likely to trust and accept AI systems.

These concerns create the need for meaningful human oversight over AI systems, particularly of those systems making high-stakes decisions, such as medical diagnoses. As noted previously, there are concerns that AI could become uncontrollable if it is granted unchecked autonomy. As AI develops, human beings must therefore remain ultimately accountable by retaining the ability to audit decisions and override them as warranted. Human-in-the-loop systems are especially important for high-risk real-time applications. In addition, all AI systems should have clearly defined constraints aligned with ethics and legal compliance. Ongoing human evaluation, even if not real-time oversight, is necessary for responsibly developing and deploying AI.

25 Anoop Krishnan and Ajita Rattani, "A Novel Approach for Bias Mitigation of Gender Classification Algorithms Using Consistency Regularization," *Image and Vision Computing*, 137 (September 2023): 104793, https://doi.org/10.1016/j.imavis.2023.104793

Advancing AI transparency, explainability, and oversight raises technical challenges. Practices such as counterfactual testing and adversarial attacks can uncover limitations and biases of the AI models being used. But these practices require specialized expertise and added complexity. Through the use of extensive testing and validation procedures, emerging techniques like “Trustworthy AI” and “AI Safety” aim to make such capabilities intrinsic to system design, not afterthoughts.

Getting governance right also involves grappling with some of the gray areas where it can be trickier to determine the appropriate actions. Without adequate safeguards, transparency could potentially open systems to gaming or manipulation by giving access to hackers and others who misuse AI. Explainability methodologies have technical limitations and assumptions that may yield explanations that are not easily understood. Furthermore, human oversight risks incorrect rejection of valid AI decisions due to cognitive biases. Strategies accounting for such subtleties are critical; oversight should focus on human strengths like **values alignment**, which involves using a shared set of values and goals approved by stakeholders to guide policies and procedures, such as AI development. These types of holistic approaches foster accountable innovation.

Meaningful oversight extends beyond internal testing to external regulation and standards. Governments must keep pace with technological change and provide appropriate legal guidance for AI development and use. This may necessitate new data protection, algorithmic accountability, and AI safety regulations. Global coordination to harmonize AI governance across borders is also important. The nonprofit International Association of Privacy Professionals maintains a Global AI Law and Policy Tracker to identify AI governance legislations all over the world.[26] They also sponsor the annual Global Privacy Summit to bring leaders from AI governance and privacy areas together. Industry leaders should collectively establish technical and ethical norms that go beyond the minimum legal requirement to help create responsible AI systems.

CAREERS IN IS

AI Ethicist

An AI ethicist analyzes technological impacts and advocates for policies that align innovations with human values. AI ethicists are concerned with the various ethical facets of AI development and product implementation, including ethical guidance and standards. They review AI policies and procedures to ensure compliance with ethical requirements. They also identify risks and recommend changes as needed to address advancements in AI.

While still fairly new, AI ethicist positions can be found in any type of organization that uses AI in its operations, including businesses, governments, and nonprofit organizations. AI ethicists work with organizational and community leaders to advocate for responsible, ethical AI development and implementation. Aspiring AI ethicists need interdisciplinary skills in technology, ethics, law, and social sciences, which enable them to gain nuanced perspectives on challenges like algorithmic bias, transparency, and worker displacement. To prepare for these roles, interested students should pursue degrees in computer science, information technology, and related fields with an emphasis on ethics and social sciences.

26 “Global AI Law and Policy Tracker,” IAPP, last updated November 2024, https://iapp.org/resources/article/global-ai-legislation-tracker/

12.4 Ethics in Health Informatics

Learning Objectives

By the end of this section, you will be able to:

- Describe the ethical use, governance, and regulation of artificial intelligence and machine learning in health care
- Identify concepts in data ownership and control of health data
- Describe the importance of privacy and confidentiality of sensitive health information

Integrating information systems and cutting-edge technologies like AI into health care presents immense opportunities and significant ethical challenges. As these digital tools reshape medicine and the patient experience, thoughtful governance and deliberation around emerging issues are critical. Key ethical considerations pertaining to health informatics include using AI responsibly, protecting sensitive data, upholding privacy and accessibility, and promoting equity.

Advances in AI, predictive analytics, telehealth, and medical devices offer new horizons for improving both quality and availability of care. At the same time, these technologies introduce risks such as inadequate data security, algorithmic bias, dehumanization of care, and unequal access. Developing appropriate oversight frameworks, aligning innovations with patient rights, and considering social implications are vital. A holistic, humanistic approach can allow health-care technology to enhance clinical judgment and person-centered care rather than replace them.

Additionally, as health care generates ever-increasing amounts of digital data, safeguarding patient privacy and confidentiality grows increasingly complex and vital. Providing adequate cybersecurity protections, complying with responsible data-sharing standards, and respecting individuals' control over their health information are essential functions. At the intersection of technology and care, trust and dignity must be paramount. With patient well-being at the center, health informatics can strengthen the bonds of compassion and humanity that define quality health care.

Ethical Governance and Regulation of Artificial Intelligence in Health Care

Integrating AI and machine learning into health care opens new frontiers for improving patient outcomes, expanding access, and revolutionizing medical science. For example, AI can be applied to data used in medical tests to diagnose diseases more accurately and more quickly, helping patients receive earlier treatment that could save lives. Artificial intelligence can also be used in datasets that support drug research and development, helping scientists better understand the genetic and biological disparities that lead to diseases and the medicines needed to address these. Artificial intelligence can also help health-care facilities with inventory management, improving efficiencies to ensure that they have necessary medications and other resources on hand to provide timely treatment to patients.

However, as AI provides exciting opportunities to improve health care, it also raises complex ethical considerations surrounding transparency, accountability, privacy, bias, and oversight. Responsible governance and regulations tailored for health AI will be imperative as these technologies continue permeating clinical settings and medical research.

Foremost, health AI systems must uphold principles of accountability and responsibility. Liability frameworks should clearly delineate where the fault lies if AI decisions or recommendations result in patient harm. Thorough validation testing and clinician oversight can help ensure safety and prevent overreliance on AI. Developers and providers must document capabilities and limitations to establish appropriate trust in AI tools. Such transparency allows clinicians to assess when AI augmentation is appropriate.

As health data processing becomes increasingly automated and vast in scope, it is important to protect

patient privacy, which provides an individual with freedom from unauthorized access and use of one's personal health information. Robust **de-identification** to remove any personal information included in data, access controls, encryption, and compliance procedures can secure personal records from unauthorized use or disclosure. Consent protocols should clearly convey how data are shared and used. Data minimization principles should ensure that data collection is limited and gathers only the data necessary to provide care. Additionally, individuals should be able to access their records and correct inaccuracies. Such measures build patient trust and prevent misuse. However, privacy protections should be designed so that they do not obstruct beneficial data sharing to conduct public health analysis or pursue research breakthroughs enabled by big data. To this end, anonymization techniques can help prevent misuse while still allowing aggregation for the common good.

Another key issue associated with health-care AI involves reducing algorithmic bias and ensuring equity in health AI design, development, and deployment. Algorithmic bias can impact the ability of the health-care industry and other institutions to provide equitable services. The following are causes for algorithmic bias:

- underrepresentation in training samples
- mislabeled outcomes
- programmers and developers who are biased
- inadequate feedback loops to identify bias

Since the data used to train AI systems often reflect social inequities, AI risks exacerbating health-care disparities if these inequities are not proactively addressed. Testing systems on diverse patient populations and representative data helps reveal bias.[27] Meanwhile, development teams from diverse backgrounds can help reveal weaknesses. Engagement with stakeholders also provides feedback on how AI impacts different groups. With concerted effort, AI can help reduce, not amplify, health-related inequality.

Realizing the safe and ethically sound potential of health AI requires balanced policymaking. Governments must develop sector-specific regulations addressing risks like breached data privacy or biased algorithms in medical devices. International coordination can help harmonize legal standards across global markets. Meanwhile, industry collaboration can establish operational best practices and technical standards exceeding legal minimums. This multitiered governance approach allows appropriate oversight without stifling innovation. In addition to top-down regulations, bottom-up advocacy is crucial. Patient groups, digital rights organizations, and other civil society stakeholders can voice concerns, advise institutions, and promote ethical norms around emerging technologies. Their on-the-ground perspectives generate important insights for human-centric and inclusive governance that works to protect all patients, including those from underrepresented and marginalized groups. This ongoing multistakeholder dialogue ensures health-care AI evolves responsibly.

CAREERS IN IS

Clinical Informatics Nurse Specialists

Clinical informatics nurse specialists analyze and implement technologies that improve health-care delivery and patient records management. For example, they assess technology and information system needs in health care, develop policies to guide the implementation and use of technology in health care, assist health-care managers with interpreting data and using them in patient care, and coordinate training sessions to teach colleagues how to use new technology. To become a clinical informatics nurse specialist, students need at least a bachelor's degree in nursing, and many students opt to earn a master's degree in nursing. They also must earn the Informatics Nursing Certification offered by the American Nurses Credentialing Center. Strong information technology, analytics, data literacy, and communication skills

27 Natalia Norori, Qiyang Hu, Florence Marcelle, Aellen, Francesca Dalia Faraci, Athina Tzovara, "Addressing Bias in Big Data and AI for Health Care: A Call for Open Science," *Patterns*, 2, no. 10 (October 8, 2021): 100347, https://doi.org/10.1016/j.patter.2021.100347

enable these health-care practitioners to be leaders as health-care facilities implement and use technology, including AI.

Implementing AI in health care requires a holistic approach that balances the technical capabilities of this technology with social responsibilities. With patient well-being at the center, transparent and compassionate design can augment, not displace, humanistic care. If guided by wisdom and proper intention, health-care AI technologies can help heal on a societal scale.

Data Ownership and Control of Health Data

As health care embraces digitization, vast quantities of sensitive patient data are being generated and analyzed. In light of this, upholding data ownership rights and enabling individuals to control how their health information is utilized has become imperative. Beyond being an ethical obligation, building trust with patients and helping them be proactive participants in their health care are foundational to realizing the full potential of data-driven medicine.

At the most basic level, the principle that patients—not providers or technology vendors—own their medical data must be respected. Custodians like hospitals and insurers possess health data, but they do not own the information. Furthermore, patients should be able to access their complete records, get copies, and move them between providers. Consent protocols must clearly convey how patients' health data will be utilized, both for care and any secondary uses like research or analytics, and must allow patients to permit or deny access. Fundamental to an ethical approach, **patient agency** secures an individual's right to access their health records, direct how their data are used, and be informed of data-sharing practices under clear consent protocols.

In practice, however, sole emphasis on consent creates difficulties. Lengthy disclosures can confuse patients, and most will not voluntarily share data unless there is a personal need to do so. This limits benefits to the larger world. Alternative models like dynamic permission, where patients can modify access in centralized databases, help balance individual control with broader societal good. In any case, consent and permission require ongoing refinement to truly empower patients.

Alongside consent, robust data protections are integral to maintaining trust. Breaches of medical records can inflict lasting harm by exposing sensitive diagnoses or genomic data. Strong cybersecurity defenses, access controls, and accountability procedures safeguard against misuse. De-identification and data minimization techniques also limit risks from unauthorized access, and transparency about security policies and data-sharing practices keeps patients informed.

Enabling patient control over data extends beyond medical records. Individuals should also be able to voluntarily share additional data like wearable readings and lifestyle information with providers. Patient-facing apps allowing such integrations and other data donations enhance agency, but they require thoughtful design regarding consent and privacy protections to prevent misuse.

Control is much less effective without health data literacy. Individuals cannot meaningfully authorize data usage when they do not understand the benefits and risks. Public outreach with educational materials and physician guidance must address such issues. Health systems should also offer patient data management portals with resources that enable them to exercise control based on preferences.

Finally, governance frameworks must evolve to reinforce patient data rights. Explicitly encoding patient ownership and control can affirm these principles. Policies should also incentivize designing for consent, portability, and interoperability. Penalties for data misuse ensure that patient rights precede institutional or commercial interests. Putting people at the center of data governance propels ethical innovation.

Privacy and Confidentiality of Sensitive Health Information

Safeguarding the privacy and confidentiality of patient health data is both an ethical obligation and a practical necessity for quality health care. As medical records become digital, ensuring information security and responsible data governance will only grow in importance. Core considerations around access controls, de-identification, bias prevention, and equity promotion form the foundation of trustworthy health-care information technology systems.

At its core, preserving privacy means controlling access to sensitive personal information. Role-based access policies, robust authentication protocols, and auditing capabilities help prevent unauthorized viewing or use of records. Additional safeguards like encryption and network segregation provide layered security, and transparency regarding security programs and breaches helps maintain patient trust. De-identification techniques are also necessary when analyzing datasets for secondary purposes like research or public health initiatives. Anonymizing data by removing obvious identifiers protects subjects' privacy without sacrificing analytic utility.

Technical measures are only one facet of privacy. Equally important are responsible policies guiding health data usage. Data minimization principles limit collection and sharing to the minimum necessary for providing care, preventing needless exposure, and consent protocols give patients control over secondary uses. Furthermore, sound oversight governance ensures adherence to these ethical data practices.

A distinct but related issue is preventing algorithmic bias and inequity resulting from flawed analytics. Since health data often reflects broader social biases, AI risks amplifying discrimination in areas like insurance eligibility if unchecked. Continual bias testing is thus essential, and human oversight of analytics is invaluable for the ethical interpretation of the data. Artificial intelligence should be an adjunct to human discernment, not a replacement.

On a societal level, policies must also evolve to reinforce health data protections in the digital age. Regulations often focus on providers and payers, leaving individual rights unclear. Laws should encode patient ownership, control, and privacy at their core. Requirements like **interoperability**, the ability of computer systems and software to exchange and make use of information through standardized formats and communication protocols, strengthens autonomy for individuals.

New approaches may be needed for ethically harnessing health data at scale while respecting rights. Options like **data collaboration**, which pools data from multiple sources, allow voluntary member data sharing for the common good under sound governance.[28] Distributed analytics and federated learning models preserve data control and minimize access. Initiatives to rectify historical exclusions and mistrust are imperative for just datasets and equitable advancement.

Understanding both the promise and principles of health-care information technology requires continuously aligning innovations with enduring human values. Patient privacy and dignity can remain inviolable with holistic policies and deliberative design. Harnessing the power of data for social good becomes possible when this process is grounded in ethics.

GLOBAL CONNECTIONS

Global Digital Health Networks

The World Health Organization coordinates worldwide digital health strategies and standards through initiatives like the Global Digital Health Partnership. Such international collaboration allows sharing best practices to strengthen health information systems equitably across nations. It facilitates technology

28 "Health Data Collaborative," Global Partnership for Sustainable Development Data, accessed January 13, 2025, https://www.data4sdgs.org/partner/health-data-collaborative

capacity building and regulation harmonization, aiming to spread benefits globally. For instance, common policy frameworks can help standardize electronic health record management across borders. Partnerships between countries enable the pooling of scarce expertise. With cooperation guiding progress, global health tech networks promote digital systems advancing care.

Key Terms

adversarial debiasing process to ensure AI is not biased by training examples

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) trade agreement setting intellectual property rights standards for member nations

copyright law legal protection granted to authors of original creative works, giving them exclusive rights to reproduce, distribute, publicly display/perform, and make derivative works for a limited time

corporate social responsibility (CSR) inherent recognition of the ethical relationship between a corporation and the larger social and environmental system that it inhabits

dark patterns deceptive interfaces that nudge users toward harmful actions, such as buying overpriced products

data collaboration process of pooling data from multiple sources

de-identification technique for removing or obscuring personal identifiers in data to protect privacy while maintaining analytic utility

deontology normative ethical theory that focuses on the inherent rightness or wrongness of actions themselves, as opposed to the consequences of those actions; follows the premise of the Golden Rule

DIKW pyramid hierarchy used in information management and knowledge creation that represents an approach focused on the distinction between disparate elements; the base of the hierarchy is data, moving up through information and knowledge to its top point of wisdom

ethical consumption being aware of the impact of consumption and making choices that prioritize longevity, repairability, and efficiency

ethics values and principles that guide life decisions and experiences

explainability ability to explain the rationale behind algorithmic predictions or automated decisions in intelligible ways to human users

fair use legal doctrine that permits limited use of copyrighted material without the copyright owner's permission for purposes such as education or news reporting

Green IS information systems practices designed to minimize ecological impacts through energy efficiency, renewable resourcing, and responsible waste disposal

human control maintaining meaningful human oversight and authority over AI systems rather than allowing fully autonomous operation; this is especially critical for high-stakes functions

human-in-the-loop system system that involves human contributions and feedback when interacting with AI

intellectual property law area of law concerned with ideas, including technological concepts; it covers trademarks, trade secrets, patents, and copyrights

interoperability ability of computer systems and software to exchange and make use of information through standardized formats and communication protocols

Lean IS information systems practices focused on eliminating redundancies and waste to optimize system efficiency and productivity

minority oversampling ensures balanced classes and sample sizes for AI training

multistakeholder collaboration process of varied stakeholders working together to achieve common goals

open-source in computing, the source code of a program open to everyone rather than being restricted via copyright

patent law legal protection granted for a limited time to inventors of new, useful, and nonobvious products or processes, giving them rights to prevent others from making, using, or selling the invention

patient agency individual's right to access their health records, direct how their data are used, and be informed of data-sharing practices under clear consent protocols

patient privacy freedom from unauthorized access to and use of one's personal health information; a right protected through data security and governance policies

sustainability long-term viability of systems, considering their environmental, economic, and social impacts

sustainable consumption and production (SCP) using and producing goods and services in a way that has the least negative impact on the environment

Sustainable Development Goals (SDGs) set of seventeen interconnected objectives established by the United Nations in 2015 to address global challenges and ensure a more sustainable future for humanity

Sustainable IS holistic approach that considers the long-term impacts and viability of information systems, focusing on environmental, economic, and social implications

sustainable supply chain management (SSCM) approach that seeks to infuse sustainability principles into the supply chain process

systems thinking perspective emphasizing the interconnectedness of components within a whole, suggesting that the overall behavior of a system results from these interactions

trade dress unique visual appearance of a product or its packaging

trade secret law business information that derives value from being kept confidential, is subject to reasonable efforts to maintain secrecy, and gives a competitive advantage

trademark law word, phrase, symbol, design, or combination thereof that identifies the source of a good or service and distinguishes it from others

utilitarianism normative ethical theory holding that the morally correct course of action is the one that maximizes utility and happiness for the greatest number of people

values alignment using a shared set of values and goals approved by stakeholders to guide policies and procedures, such as AI development

virtue ethics normative ethical approach emphasizing the embodiment of virtues and ideals as the path toward an ethical, flourishing life

World Intellectual Property Organization (WIPO) UN agency that promotes IP protection and cooperation between nations to foster innovation and creativity

Summary

12.1 Ethics, Sustainability, and Use of Information Systems

- Three main normative theories provide frameworks for assessing the ethics of actions: utilitarianism, which focuses on consequences of actions; deontology, which evaluates the action itself; and virtue ethics, which concentrates on the character of the actor.
- Systems thinking enhances ethical reasoning by emphasizing holistic analysis of complex situations' interconnected components and relationships. This allows for a broader understanding of direct and indirect impacts.
- Sustainability considers the long-term viability of organizational systems in terms of environmental stewardship, economic viability, and social welfare. Information systems practices should align with these sustainability pillars to minimize waste and harsh effects on the environment, increase efficiencies in business, and promote a positive impact on society.
- Green IS focuses on minimizing information systems' ecological footprint through energy efficiency, renewable resourcing, responsible disposal, and similar practices.
- Lean IS concentrates on eliminating information system waste and redundancies to optimize productivity, efficiency, and resource utilization.
- Sustainable IS provides a more holistic approach, considering information systems' long-term impacts and viability, focusing on environmental, economic, and social implications.
- Sustainable supply chain management seeks to infuse sustainability principles into the supply chain process.
- Corporate social responsibility is an inherent recognition of the ethical relationship between a corporation and the larger societal and environmental system that it inhabits. Companies can use the three Ps of CSR (people, planet, profit) as a guide to determine appropriate information system and technology practices to follow.
- As information systems become more integrated into society, thoughtful application of ethical frameworks

and sustainable practices will be crucial for responsible innovation that benefits humanity.

12.2 Intellectual Property

- The United States recognizes four forms of IP, and each is protected by its own law: copyrights, patents, trade secrets, and trademarks. These forms of IP law provide legal protections for a period of time to incentivize the creation of new information.
- Each form of IP has different requirements to initiate or apply for protection, as well as different protections provided, and varying durations.
- Each of these forms of IP has the potential to provide monetary rewards for organizations that employ information systems and information technology.
- Intellectual property laws raise ethical issues. For example, they have the potential to restrict access to information and technology, which can create a digital divide. Individuals and communities that lack access may experience disadvantages if they cannot use this information and technology for things such as decision-making.
- There are several international initiatives that seek to protect IP. These generally seek to harmonize existing IP laws across national borders to make IP function more uniformly and efficiently for companies that operate in multiple nations.

12.3 Ethics of Artificial Intelligence Development and Machine Learning

- Responsible AI development includes ethical governance that addresses considerations such as transparency, accountability, bias prevention, human control, and oversight. Regulations and industry standards ensure that technology is aligned with human values and principles.
- Multistakeholder collaboration between governments, companies, and civil society is critical to developing policies and norms that can effectively govern the growth of ethical AI innovation.
- Algorithmic bias must be proactively addressed through testing that involves diverse datasets, audits, minority oversampling, and human monitoring. Transparency regarding AI development builds trust with users.
- Explainability methodologies provide insight into AI decision logic. Continual human validation and oversight are essential, especially for high-stakes decisions.

12.4 Ethics in Health Informatics

- The use of AI and automation in health care requires thoughtful governance that addresses accountability, privacy, security, bias prevention, and human oversight to ensure responsible innovation. Regulations and policies must balance emerging technologies with patient rights.
- Upholding individual control and consent regarding health data usage builds patient trust and prevents misuse, while still allowing ethical data sharing for the public good.
- Safeguarding the privacy of sensitive patient information requires robust technical protections such as access controls, encryption, and de-identification, as well as responsible data governance policies.
- Algorithmic bias and systemic discrimination must be proactively addressed to promote health equity. Inclusive design and community engagement foster the ethical use of technology.
- With patient well-being at the core, innovations like AI can be harnessed to augment—not replace—humanistic health care. Ethical governance and compassionate design are imperative.

Review Questions

1. What ethical theory focuses on taking actions that could be universalized as moral laws that all individuals should follow?
   a. virtue ethics
   b. utilitarianism
   c. deontology
   d. consequentialism

2. What is the main principle of utilitarianism?
    a. create the greatest good for the greatest number
    b. only take actions that you would want others to take
    c. develop virtues to become an ideal human being
    d. focus on the consequences of actions
3. Systems thinking emphasizes the importance of viewing components as part of a larger, interconnected ________.
    a. process
    b. goal
    c. team
    d. whole
4. What practice involves eliminating redundancies and waste to improve efficiency in information systems?
    a. Green IS
    b. Lean IS
    c. Secure IS
    d. Sustainable IS
5. What type of intellectual property protection is best suited for a company logo?
    a. copyright
    b. patent
    c. trademark
    d. trade secret
6. What does the World Intellectual Property Organization (WIPO) primarily do?
    a. protects individual copyrights globally
    b. prosecutes international patent infringements
    c. promotes the protection of IP rights worldwide
    d. assigns internet domain names
7. In the context of IP law, what term best describes the protection of information that a company wishes to keep secret, such as a proprietary recipe or manufacturing process?
    a. copyright
    b. patent
    c. trademark
    d. trade secret
8. What form of intellectual property law would prevent a competitor from reverse engineering a new process for integrating information systems into a corporate setting?
    a. copyright
    b. patent
    c. trademark
    d. trade secret
9. What practice involves continually testing AI systems using diverse datasets to reveal inaccurate preconceptions?
    a. encryption
    b. transparency
    c. bias testing
    d. accountability
10. What concept refers to the ability to describe an AI model's logic and decisions in understandable ways?
    a. constraining

b. governance
c. explainability
d. anonymization

11. Who should ultimately remain responsible for high-stakes decisions being informed by AI?
    a. the AI system
    b. government regulators
    c. company executives
    d. human overseers

12. What term describes the openness and visibility into how an AI system functions?
    a. explainability
    b. transparency
    c. equity
    d. oversight

13. What practice helps ensure AI systems complement humans rather than replace human discretion?
    a. automated decision-making
    b. accountability
    c. technological unemployment
    d. human control

14. What concept refers to an individual's right to access and control their health data?
    a. interoperability
    b. patient privacy
    c. consent
    d. patient agency

15. What technique involves removing specific details from patient data to protect privacy?
    a. encryption
    b. immutability
    c. anonymization
    d. de-identification

16. Who should remain ultimately responsible for high-risk clinical decisions informed by artificial intelligence?
    a. the AI system
    b. government regulators
    c. hospital administrators
    d. human health-care providers

17. What practice helps ensure underserved communities can access health technologies?
    a. liability insurance
    b. discrimination testing
    c. digital literacy initiatives
    d. inclusive design

Check Your Understanding Questions

1. What is systems thinking and how can it be useful in ethical decision-making?
2. What are the three pillars of sustainability in information systems?
3. Explain the requirements a work needs to meet to gain copyright protection.
4. Describe the role of the World Intellectual Property Organization.

5. Why are trademarks important in the information systems industry?
6. How can algorithmic bias be mitigated when developing AI systems?
7. Why is explainability important for ethical AI systems?
8. What role does multistakeholder collaboration play in ethical AI governance?
9. How does robust data governance help uphold patient privacy in health-care information systems?

Application Questions

1. How might your ethical perspective change when assessing a situation from an individual versus organizational versus societal perspective? What factors might you prioritize differently?
2. Reflect on a recent technological innovation that you find interesting. Considering what you have learned about intellectual property law, how would you protect this innovation from being copied or stolen? What type of intellectual property protection (copyright, patent, trademark, trade secret) would be most suitable and why? Discuss any potential challenges or issues that could arise in protecting this innovation and how you might address them.
3. Think of an AI or automated system you regularly use. What potential ethical risks or biases might it have that you could investigate further? How could you envision enhancing transparency or human oversight?
4. Watch the video overview of IBM's AI FactSheets (https://openstax.org/r/109AIFactSheet) on its practices. How could Supplier Declaration of Conformity fact sheets help promote ethical AI governance? What limitations might exist?
5. How would you want health-care technologies like artificial intelligence or big data analytics to be used in your own medical care? What concerns would you have?
6. How might your perspective on health data privacy change if you or a loved one relied on connected technologies like pacemakers or glucose monitors? What concerns might emerge?

Answer Key

Chapter 1

Review Questions

1. b
3. a
5. d
7. d
9. c
11. d
13. b
15. c
17. a

Chapter 2

Review Questions

1. c
3. d
5. c
7. a
9. b
11. d

Chapter 3

Review Questions

1. b
3. c
5. c
7. a
9. a

Chapter 4

Review Questions

1. b
3. d
5. b
7. d
9. b
11. c
13. b
15. c
17. b

Chapter 5

Review Questions

1. b

3. c
5. c
7. c
9. b
11. b
13. c
15. c
17. b
19. b
21. c

Chapter 6

Review Questions

1. a
3. a
5. b
7. a
9. c
11. b
13. b
15. c
17. b
19. c

Chapter 7

Review Questions

1. a
3. c
5. a
7. c
9. b
11. a
13. c
15. a
17. b
19. c
21. a
23. c
25. d

Chapter 8

Review Questions

1. b
3. d
5. a
7. b
9. c

11. c
13. d
15. c
17. c

Chapter 9

Review Questions

1. a
3. c
5. a
7. a
9. a

Chapter 10

Review Questions

1. a
3. b
5. d
7. b
9. a
11. d

Chapter 11

Review Questions

1. b
3. c
5. d
7. c
9. a
11. b
13. c
15. b

Chapter 12

Review Questions

1. c
3. d
5. c
7. d
9. c
11. d
13. d
15. d
17. d

Index

G

H

I