PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Cert Guide

Advance your IT career with hands-on learning

CISSP

Fifth Edition

ROBIN ABERNATHY
Dr. DARREN R. HAYES

FREE SAMPLE CHAPTER |

CISSP Cert Guide, Fifth Edition

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **www.pearsonitcertification.com/register**.
2. Enter the **print book ISBN**: 9780135343999.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

This page intentionally left blank

CISSP Cert Guide

Fifth Edition

Robin M. Abernathy
Dr. Darren R. Hayes

Pearson

Hoboken, New Jersey

CISSP Cert Guide, Fifth Edition

Please contact us with concerns about any potential bias atpearson.com/report-bias.html.

ISBN-13: 978-0-13-534399-9

ISBN-10: 0-13-534399-2

Library of Congress Control Number: 2024911820

$PrintCode

GM K12, Early Career and Professional Learning
Soo Kang

Product Line Manager
Brett Bartow

Executive Editor
James Manly

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Mandie Frank

Copy Editor
Bill McManus

Indexer
Timothy Wright

Proofreader
Donna E. Mulder

Technical Editors
R. Sarma Danturthi
Ben Mayo

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Online Elements

Table of Contents

Online Elements

About the Authors

Robin M. Abernathy has been working in the IT certification preparation industry for more than 20 years. She has written and edited certification preparation materials for many $(ISC)^2$, Microsoft, CompTIA, PMI, ITIL, ISACA, and GIAC certifications and holds multiple IT certifications from these vendors.

Robin provides training on computer hardware and software, networking, security, and project management. Over the past decade, she has ventured into the traditional publishing industry by technically editing several publications and co-authoring Pearson's *CISSP Cert Guide* and *CASP+ Cert Guide* and authoring Pearson's *Project+ Cert Guide*. She presents at technical conferences and hosts webinars on IT certification topics.

Dr. Darren R. Hayes has close to 20 years of academic and professional experience in computer security and digital forensics. He has authored numerous publications in these fields, including *A Practical Guide to Digital Forensics Investigations*, which is published by Pearson. He is Associate Professor at Pace University, where he is the founder and director of the Seidenberg Digital Forensics Research Lab. He holds numerous IT certifications in security and digital forensics and holds a PhD from Sapienza University in Italy and a doctorate from Pace University.

Darren is also a professional digital forensics examiner and has supported both criminal and civil investigations over the past decade and a half. He has also been declared an expert witness in federal court.

Dedications

To all those out there on a certification journey!

—Robin

To all our cyber warriors who protect our businesses and our national security. Your careers are so demanding and your ambition to gain certifications is to be commended.

—Darren

Acknowledgments

My first thanks goes to God for blessing me with the ability to learn and grow in any field I choose. With Him, all things are possible!

For me, it is hard to believe that I am on the fifth edition of this book. I appreciate my family and my friends, who have supported me in my publishing journey through three titles and multiple editions.

It is my hope that you, the reader, succeed in your IT certification goals!

—Robin

To my beautiful wife, Nalini, and my children, Aine, Fiona, Nicolai, and Shay, I cannot thank you enough for your support and love over the years. Also, to my parents, Ted and Annette, who inspired me to be an eternal learner and try to help others to gain knowledge. I would like to acknowledge my fellow teachers who make immeasurable sacrifices to see their students succeed. My sincere thanks to all of the tremendous reviewers, editors, and other staff at Pearson whom I have had the honor of working with for many years.

—Darren

About the Technical Reviewers

R. Sarma Danturthi, PhD, PMP, CISSP, has a doctoral degree in engineering from the University of Memphis, Memphis, Tennessee, and has taught graduate-level courses in engineering, microprocessors, and computer science. He has been in the IT field for more than 20 years. His earlier experience included designing processor-level boards with interfaces and programming with several languages such as C and C++ on various platforms such as Windows, Linux, UNIX, and VAX/VMS. He has been a funding proposal reviewer, scientific paper peer reviewer for universities in the USA and Taiwan, book reviewer and exam preparation subject matter expert for Pearson, $(ISC)^2$, and CompTIA.

His current experience includes information and cybersecurity, database security, software and application security, project team lead, and project management. He has published several papers in peer-reviewed journals and has written book chapters on software interfaces, modeling, IT security, and simulation. His interests include evolving cybersecurity, cloud computing, intelligent interfaces, and mobile application development. Besides being proficient in various programming languages, databases, information, and cybersecurity, he has certifications in Java, Project Management Institute's PMP, CompTIA Sec+, and $(ISC)^2$'s CISSP.

Dr. Danturthi published *70 Tips and Tricks for Mastering the CISSP Exam* (Apress) in 2020. He can be contacted at danturthi@gmail. com.

Ben Mayo, CCIE No. 24861, CISSP, is the head of security and lead engineer for Montana's largest independent network and data center provider. He has more than 19 years of experience in the network and security fields. Ben's experience spans multiple industries, including electrical power generation, education, and telecommunications. Ben takes a "purple team" approach to security, applying both offensive and defensive security practices to enhance his organization's security posture. Though security is his passion, he most enjoys spending time with his three awesome kids and his amazing wife. You can follow Ben on Twitter at @ping_18024.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *CISSP Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account.* Enter the product ISBN 9780135343999 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Certified Information Systems Security Professional (CISSP) is one of the most respected and sought-after security certifications available today. It is a globally recognized credential, which demonstrates that the holder has knowledge and skills across a broad range of security topics.

As the number of security threats to organizations grows and the nature of these threats broadens, companies large and small have realized that security can no longer be an afterthought. It must be built into the DNA of the enterprise to be successful. Consequently, trained professionals must be versed not only in technology security but all aspects of security. It also requires a holistic approach to protecting the enterprise.

Security today is no longer a one-size-fits-all proposition. The CISSP credential is a way security professionals can demonstrate the ability to design, implement, and maintain the correct security posture for an organization, based on the complex environments in which today's organizations exist.

The Goals of the CISSP Certification

The CISSP certification is created and managed by one of the most prestigious security organizations in the world and has a number of stated goals. Although not critical for passing the exam, having knowledge of the organization and of these goals is helpful in understanding the motivation behind the creation of the exam.

Sponsoring Bodies

The CISSP is created and maintained by the International Information System Security Certification Consortium $(ISC)^2$. The $(ISC)^2$ is a global not-for-profit organization that provides both a vendor-neutral certification process and supporting educational materials.

The CISSP is one of a number of security-related certifications offered by $(ISC)^2$. Other certifications offered by this organization include the following:

- Systems Security Certified Practitioner (SSCP)
- Certified Cloud Security Professional (CCSP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Life Cycle Professional (CSSLP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)

Several additional versions of the CISSP are offered that focus in particular areas:

- CISSP-Information Systems Security Architecture Professional (CISSP-ISSAP)
- CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)
- CISSP-Information Systems Security Management Professional (CISSP-ISSMP)

$(ISC)^2$ derives some of its prestige from the fact that it was the first security certification body to meet the requirements set forth by ANSI/ISO/IEC Standard 17024, a global benchmark for personnel certification. This ensures that certifications offered by this organization are both highly respected and sought after.

Stated Goals

The goal of $(ISC)^2$, operating through its administration of the CISSP and other certifications, is to provide a reliable instrument to measure an individual's knowledge of security. This knowledge is not limited to technology issues alone but extends to all aspects of security that face an organization.

In that regard, the topics are technically more shallow than those tested by some other security certifications, while also covering a much wider range of issues than those other certifications. Later, we cover the topics that comprise the eight domains of knowledge in detail, but it is a wide range of topics. This vast breadth of knowledge and the experience needed to pass the exam are what set the CISSP certification apart.

The Value of the CISSP Certification

The CISSP certification holds value for both the exam candidate and the enterprise. This certification is routinely in the top 10 of yearly lists that rank the relative demand for various IT certifications.

To the Security Professional

A security professional would spend the time and effort required to achieve this credential for numerous reasons:

- To meet growing demand for security professionals
- To become more marketable in an increasingly competitive job market
- To enhance skills in a current job

- To qualify or compete more successfully for a promotion
- To increase salary

In short, this certification demonstrates that the holder not only has the knowledge and skills tested in the exam but also has the wherewithal to plan and implement a study plan that addresses an unusually broad range of security topics.

To the Enterprise

For an organization, the CISSP certification offers a reliable benchmark to which job candidates can be measured by validating knowledge and experience. Candidates who successfully pass the rigorous exam are required to submit documentation verifying experience in the security field. Individuals holding this certification will stand out from the rest, not only making the hiring process easier but also adding a level of confidence in the final hire.

The Common Body of Knowledge

The material contained in the CISSP exam is divided into eight domains, which comprise what is known as the Common Body of Knowledge. This book devotes a chapter to each of these domains. Inevitable overlap occurs between the domains, leading to some overlap between topics covered in the chapters; the topics covered in each chapter are described next.

Security and Risk Management

The Security and Risk Management domain, covered in Chapter 1, encompasses a broad spectrum of general information security and risks management topics and is 15 percent of the exam. Topics include

- Professional ethics
- Concepts of confidentiality, integrity, availability, authenticity, and nonrepudiation
- Security governance principles
- Compliance requirements
- Legal and regulatory issues
- Investigation types
- Security policy, standards, procedures, and guidelines
- Business continuity (BC) requirements

- Personnel security policies and procedures
- Risk management concepts
- Threat modeling concepts and methodologies
- Supply chain risk management (SCRM) concepts
- Security awareness, education, and training program

Asset Security

The Asset Security domain, covered in Chapter 2, focuses on the collection, handling, and protection of information throughout its life cycle and is 10 percent of the exam. Topics include

- Information and asset identification and classification
- Information and asset handling requirements
- Resource provisioning
- Data life cycle
- Asset retention
- Data security controls and compliance requirements

Security Architecture and Engineering

The Security Architecture and Engineering domain, covered in Chapter 3, addresses the practice of building information systems and related architecture that deliver the required functionality when threats occur and is 13 percent of the exam. Topics include

- Engineering processes using secure design principles
- Fundamental concepts of security models
- Control selection based on systems security requirements
- Security capabilities of information systems
- Vulnerabilities of security architectures, designs, and solution elements
- Cryptography
- Cryptanalytic attacks
- Security principles of site and facility design
- Site and facility security controls

Communication and Network Security

The Communication and Network Security domain, covered in Chapter 4, focuses on protecting data in transit and securing the underlying networks over which the data travels and is 13 percent of the exam. Topics include

- Secure design principles in network architectures
- Network components security
- Secure communication channels

Identity and Access Management (IAM)

The Identity and Access Management domain, covered in Chapter 5 and comprising 13 percent of the exam, discusses provisioning and managing the identities and access used in the interaction of humans and information systems, of disparate information systems, and even between individual components of information systems. Topics include

- Physical and logical access to assets
- Identification and authentication of people, devices, and services
- Federated identity as a third-party service
- Authorization mechanisms
- Identity and access provisioning life cycle
- Authentication systems

Security Assessment and Testing

The Security Assessment and Testing domain, covered in Chapter 6 and comprising 12 percent of the exam, encompasses the evaluation of information assets and associated infrastructure using tools and techniques for the purpose of identifying and mitigating risk due to architectural issues, design flaws, configuration errors, hardware and software vulnerabilities, coding errors, and any other weaknesses that may affect an information system's ability to deliver its intended functionality in a secure manner. The topics include

- Assessment, test, and audit strategies design and validation
- Security control testing
- Security process data collection
- Test output analysis and reporting
- Security audits

Security Operations

The Security Operations domain, covered in Chapter 7, surveys the execution of security measures and maintenance of proper security posture and is 13 percent of the exam. Topics include

- Investigations compliance
- Logging and monitoring activities
- Configuration management
- Security operations concepts
- Resource protection
- Incident management
- Detective and preventive measures
- Patch and vulnerability management
- Change management processes
- Recovery strategies
- Disaster recovery (DR) processes
- Disaster recovery plan (DRP) testing
- Business continuity (BC) planning and exercises
- Physical security implementation and management
- Personnel safety and security concerns

Software Development Security

The Software Development Security domain, covered in Chapter 8, explores the software development life cycle and development best practices and is 11 percent of the exam. Topics include

- Software development life cycle (SDLC) security
- Security controls in development environments
- Software security effectiveness
- Security impact of acquired software
- Secure coding guidelines and standards

Steps to Becoming a CISSP

To become a CISSP, a test candidate must meet certain prerequisites and follow specific procedures. Test candidates must qualify for the exam and sign up for the exam.

Qualifying for the Exam

Candidates must have a minimum of five years of paid full-time professional security work experience in two or more of the eight domains in the Common Body of Knowledge. You may receive a one-year experience waiver with a four-year college degree or additional credential from the approved list, available at the (ISC)^2 website, thus requiring four years of direct full-time professional security work experience in two or more of the eight domains of the CISSP.

If you lack this experience, you can become an Associate of (ISC)^2 by successfully passing the CISSP exam. You'll then have six years to earn your experience to become a CISSP.

Signing Up for the Exam

The steps required to sign up for the CISSP are as follows:

1. Create a Pearson Vue account and schedule your exam.
2. Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience and legally committing to the adherence of the (ISC)^2 Code of Ethics.
3. Review the Candidate Background Questions.
4. Submit the examination fee.

When you are notified that you have successfully passed the examination, you will be required to subscribe to the (ISC)^2 Code of Ethics and have your application endorsed before the credential can be awarded. An endorsement form for this purpose must be completed and signed by an (ISC)^2 certified professional who is an active member and who is able to attest to your professional experience.

Facts About the CISSP Exam

The CISSP exam is a computer-based test that the candidate can spend up to three to six hours completing (depending on whether you take the CAT version that is available in English only or the linear format that is available in all other languages). There are no formal breaks, but you are allowed to bring a snack and eat it at the back of the test room, but any time used for that break counts toward the three to six hours. You must bring a government-issued identification card. No other forms of ID will be accepted. You may be required to submit to a palm vein scan.

The CAT test consists of a maximum 175 questions, while the linear format consists of 250 questions. As of May 2022, the CISSP exam will be in a computerized adaptive testing (CAT) format for those who take the English-language version, whereas all other languages have only the linear format. With the CAT format, the computer evaluates the certification candidate's ability to get the next question right based on the candidate's previous answers and the difficulty of those questions. The questions get harder as the certification candidate answers questions correctly, and the questions get easier as the certification candidate answers questions incorrectly. Each answer affects the questions that follow. Therefore, unlike the linear test format where the certification candidate can go back and forth in the question pool and change answers, a CAT format exam does *not* allow the certification candidate to change the answer or even view a previously answered question. The certification candidate may receive a pass or fail score without seeing 175 questions. To find out more about the CAT format, please go to www.isc2.org/Certifications/CISSP/CISSP-CAT#.

Although the majority of the questions will be multiple-choice questions with four options, test candidates may also encounter drag-and-drop and hotspot questions. The passing grade is 700 out of a possible 1,000 points. Candidates will receive the unofficial results at the test center from the test administrator. (ISC)^2 will then follow up with an official result via email.

About the *CISSP Cert Guide*, Fifth Edition

This book maps to the topic areas of the (ISC)^2 Certified Information Systems Security Professional (CISSP) exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization; it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the CISSP exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section lists a series of study activities that you should do at the end of the chapter:
  - **Review All Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
  - **Define Key Terms:** Although the CISSP exam may be unlikely to ask a question such as "Define this term," the exam does require that you learn and know a lot of information systems security terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
  - **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Cert Practice Test engine that allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains eight core chapters—Chapters 1 through 8. Chapter 9 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CISSP exam. The core chapters map directly to the CISSP exam topic areas and cover the concepts and technologies that you will encounter on the exam.

How to Access the Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials, as well as additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box indicating that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

Step 1. Go to **www.pearsonitcertification.com/register** and log in or create a new account.

Step 2. Enter the ISBN: **9780135343999**.

Step 3. Answer the challenge question as proof of purchase.

Step 4. Click the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps above, please visit www.pearsonITcertification.com/contact and select the Site Problems/ Comments option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software, containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions below.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- You can get your access code by registering the print ISBN (9780135343999) on pearsonitcertification.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. After you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code

are available on the book's companion website by clicking the Access Bonus Content link.

- If you purchase the Premium Edition eBook and Practice Test directly from the Pearson IT Certification website, the code will be populated on your account page after purchase. Just log in at pearsonitcertification.com, click Account to see details of your account, and click the Digital Purchases tab.

NOTE After you register your book, your code can always be found in your account on the Registered Products tab.

Once you have the access code, to find instructions about both the Pearson Test Prep web app and the desktop app, follow these steps:

Step 1. Open this book's companion website, as shown earlier in this Introduction, under the heading, "How to Access the Companion Website."

Step 2. Click the **Practice Test Software** button.

Step 3. Follow the instructions listed there for both installing the desktop app and using the web app.

Note that if you want to use the web app only at this point, just navigate to pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters; then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

Figure Credits

Figures 4.47 and 4.49: Microsoft

Figure 7.13: Ratchat/Shutterstock

This page intentionally left blank

Asset Security

Assets are any entities that are valuable to an organization and include ***tangible*** and ***intangible assets***. As mentioned in Chapter 1, "Security and Risk Management," tangible assets include computers, facilities, supplies, and personnel. Intangible assets include intellectual property, data, and organizational reputation. All assets in an organization must be protected to ensure the organization's future success. Although securing some assets is as easy as locking them in a safe, other assets require more advanced security measures. The most valuable asset of any organization is its data.

The Asset Security domain addresses a broad array of topics, including information and asset identification and classification, information and asset handling, information and asset ownership, asset inventory and asset management, data life cycle, asset retention, and data security controls and compliance requirements. Out of 100 percent of the exam, this domain carries an average weight of 10 percent, which is the lowest weight of the domains.

A security professional must be concerned with all aspects of asset security. The most important factor in determining the controls used to ensure asset security is an asset's value. Although some assets in the organization may be considered more important because they have greater value, you should ensure that no assets are forgotten. This chapter covers all the aspects of asset security that you, as an IT security professional, must understand.

NOTE Throughout this chapter, the terms *information* and *data* are used interchangeably, as commonly happens in the real world.

Foundation Topics

Asset Security Concepts

Asset security concepts that you must understand include

- Asset and data policies
- Data quality
- Data documentation and organization

Asset and Data Policies

As a security professional, you should ensure that your organization implements a data ***policy*** that defines long-term goals for data management and asset policies that define long-term goals for each asset type at a minimum. In some cases, each asset may need its own defined policy to ensure that it is properly administered. Business units will need to define asset policies and data policies for any assets and data owned by that business unit. Asset and data policies should be based on the organization's overall asset and data policies. Individual roles and responsibilities should be defined to ensure that personnel understand their job tasks as related to these policies.

After the overall policies are created, asset and data management practices and procedures should be documented to ensure that the day-to-day tasks related to assets and data are completed. In addition, the appropriate quality assurance and quality control procedures must be put into place for data quality to be ensured. Storage and backup procedures must be defined to ensure that assets and data can be restored.

As part of a data policy, any databases implemented within an organization should be carefully designed based on user requirements and the type of data to be stored. All databases should comply with the data policies that are approved, created, and implemented. Data policies should be strictly enforced.

Prior to establishing a data policy, you should consider several issues that can affect it. These issues include risks, cost, liability, legal and regulatory requirements, privacy, sensitivity, and ownership.

The cost of any data management mechanism is usually the primary consideration of any organization. Often organizations do not implement a data policy because they think it is easier to allow data to be stored in whatever way each business unit or user desires. However, if an organization does not adopt formal data policies and

procedures, data security issues can arise because of the different storage methods used. For example, suppose an organization's research department decides to implement a Microsoft SQL Server database to store all research data, but the organization does not have a data policy. If the database is implemented without a thorough understanding of the types of data that will be stored and the users' needs, the research department may end up with a database that is difficult to navigate and manage. In addition, the proper access control mechanism may not be in place, resulting in users being able to edit the data that should only have view access.

Liability involves protecting the organization from legal issues. Liability is directly affected by legal and regulatory requirements that apply to the organization. Issues that can affect liability include asset or data misuse, data inaccuracy, data corruption, data breach, and data loss or a data leak.

Data privacy is determined as part of data analysis. Data classifications must be determined based on the value of the data to the organization. After the data classifications are determined, data controls should be implemented to ensure that the appropriate security controls are implemented based on data classifications. Privacy laws and regulations must also be considered.

Sensitive data is any data that could adversely affect an organization or individual if it were released to the public or obtained by attackers. When determining sensitivity, you should understand the types of threats that can occur, the vulnerability of the data, and the data type. For example, Social Security numbers are more sensitive than physical address data.

Data ownership is the final issue that you must consider as part of data policy design. This issue is particularly important if multiple organizations store their data within the same asset or database. One organization may want completely different security controls in place to protect its data. Understanding legal ownership of data is important to ensure that you design a data policy that takes into consideration the different requirements of multiple data owners. While this is most commonly a consideration when multiple organizations are involved, it can also be an issue with different business units in the same organization. For example, data from the human resources department has different owners and therefore different requirements than research department data.

Data Quality

Data quality is defined as data's fitness for use. The integrity factor of the security triad drives the data quality. Data quality must be maintained throughout the data life cycle, including during data capture, data modification, data storage, data distribution, data usage, and data archiving. These terms are also known as *data in use*,

data at rest, and *data in transit*. Security professionals must ensure that their organization adopts the appropriate quality control and quality assurance measures so that data quality does not suffer. Data quality is most often safeguarded by ensuring data integrity, which protects data from unintentional, unauthorized, or accidental changes. With data integrity, data is known to be good, and information can be trusted as being complete, consistent, and accurate. System integrity ensures that a system will work as intended.

Security professionals should work to document data standards, processes, and procedures to monitor and control data quality. In addition, internal processes should be designed to periodically assess data quality. When data is stored in databases, quality control and assurance are easier to ensure using the internal data controls in the database. For example, you can configure a field to only a valid number. By doing this, you would ensure that only numbers could be input into the field. This is an example of input validation. Input validation can occur on both the client side (using regular expressions) and the server side (using code or in the database) to avoid SQL injection attacks.

Data ***contamination*** occurs when data errors occur. Data can be corrupt due to network or hash corruptions, lack of integrity policies, transmission errors, and bad encryption algorithms. Data errors can be reduced through implementation of the appropriate quality control and assurance mechanisms. Data verification, an important part of the process, evaluates how complete and correct the data is and whether it complies with standards. Data verification can be carried out by personnel who have the responsibility of entering the data. Data validation evaluates data after data verification has occurred and tests data to ensure that data quality standards have been met. Data validation must be carried out by personnel who have the most familiarity with the data.

Organizations should develop procedures and processes that keep two key data issues in the forefront: error prevention and correction. Error prevention is provided at data entry, whereas error correction usually occurs during data verification and validation.

Data Documentation and Organization

Data documentation ensures that data is understood at its most basic level and can be properly organized into data sets. Data sets ensure that data is arranged and stored in a relational way so that the data can be used for multiple purposes. Data sets should be given unique, descriptive names that indicate their contents.

By documenting the data and organizing data sets, organizations can also ensure that duplicate data is not retained in multiple locations. For example, the sales department may capture all demographic information for all customers. However, the

shipping department may also need access to this same demographic information to ensure that products are shipped to the correct address. In addition, the accounts receivable department will need access to customer demographic information for billing purposes. There is no need for each business unit to have separate data sets for this information. Identifying the customer demographic data set as being needed by multiple business units prevents duplication of efforts across business units.

Within each data set, documentation must be created for each type of data. In the customer demographic data set example, customer name, address, and phone number are all collected. For each of the data types, the individual parameters for each data type must be created. Whereas an address may allow a mixture of numerals and characters, a phone number should allow only numerals. In addition, each data type may have a maximum length. Finally, it is important to document which data is required—meaning that it must be collected and entered. For example, an organization may decide that fax numbers are not required but phone numbers are required. Remember that each of these decisions is best made by the personnel working most closely with the data.

After all the documentation has been completed, the data organization must be mapped out. This organization will include all interrelationships between the data sets. It should also include information on which business units will need access to data sets or subsets of a data set.

NOTE *Big data* is a term for data sets that are so large or complex that they cannot be analyzed by traditional data processing applications. Specialized applications have been designed to help organizations with their big data. The big data challenges that may be encountered include data analysis, data capture, data search, data sharing, data storage, data mining, and data privacy.

Identify and Classify Information and Assets

Security professionals should ensure that the organizations they work for properly identify and classify all organizational information and assets. The first step in this process is to identify all information and assets the organization owns and uses. To perform information and asset identification, security professionals should work with the representatives from each department or functional area. After the information and assets are identified, security professionals should perform data and asset classification and document sensitivity and criticality of data.

Security professionals must understand private sector classifications, military and government classifications, the information life cycle, databases, and data audit.

Data and Asset Classification

Data and assets should be classified based on their value to the organization and their sensitivity to disclosure. Assigning a value to data and assets allows an organization to determine the resources that should be used to protect them. Resources that are used to protect data include personnel resources, monetary resources, access control resources, and so on. Classifying data and assets allows you to apply different protective measures. Data classification is critical to all systems to protect the ***confidentiality***, ***integrity***, and ***availability*** (CIA) of data.

After data is classified, the data can be segmented based on its level of protection needed. The classification levels ensure that data is handled and protected in the most cost-effective manner possible. The assets could then be configured to ensure that data is isolated or protected based on these classification levels. An organization should determine the classification levels it uses based on the needs of the organization. A number of private sector classifications and military and government information classifications are commonly used.

NOTE The common private sector classifications and military and government classifications are discussed in a later section.

The information life cycle, covered in more detail later in this chapter, should also be based on the classification of the data. Organizations are required to retain certain information, particularly financial data, based on local, state, or government laws and regulations.

Sensitivity and Criticality

Data sensitivity is a measure of how freely data can be handled. Some data requires special care and handling, especially when inappropriate handling could result in penalties, identity theft, financial loss, invasion of privacy, or unauthorized access by an individual or many individuals. Some data is also subject to regulation by state or federal laws and requires notification in the event of a disclosure.

Data is assigned a level of sensitivity based on who should have access to it and how much harm would be done if it were disclosed. This assignment of sensitivity is called data classification.

Data criticality is a measure of the importance of the data. Data that is considered sensitive may not necessarily be considered critical. Assigning a level of criticality to a particular data set requires considering the answers to a few questions:

- Will you be able to recover the data in case of disaster?
- How long will it take to recover the data?

- How safely, accurately and quickly can an organization recover the data in case of an incident or disaster?
- What is the effect of this downtime, including loss of public standing?

Data is considered essential when it is critical to the organization's business. When essential data is not available, even for a brief period of time, or when its integrity is questionable, the organization is unable to function at its optimal level. Data is considered required when it is important to the organization but organizational operations would continue for a predetermined period of time even if the data were not available. Data is nonessential if the organization is able to operate without it during extended periods of time.

When the sensitivity and criticality of data are understood and documented, the organization should then work to create a data classification system. Most organizations either use a private sector classification system or a military and government classification system.

PII

Personally identifiable information (PII) was defined and explained in Chapter 1. PII is considered information that should be classified and protected. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122 gives ***guidelines*** on protecting the confidentiality of PII.

According to SP 800-122, organizations should implement the following recommendations to effectively protect PII:

Key Topic

- Organizations should identify all PII residing in their environment.
- Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.
- Organizations should categorize their PII by the PII confidentiality impact level.
- Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level.
- Organizations should develop an incident response plan to handle breaches involving PII.
- Organizations should encourage close coordination among their chief privacy officers, senior agency officials for privacy, chief information officers, chief information security officers, and legal counsel when addressing issues related to PII.

SP 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." To distinguish an individual is to identify an individual. To trace an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status. Linked information is information about or related to an individual that is logically associated with other information about the individual. In contrast, linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual.

All PII should be assigned confidentiality impact levels based on the FIPS 199 designations. Those designations are

- LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
- MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
- HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Determining the impact from a loss of confidentiality of PII should take into account relevant factors. Several important factors that organizations should consider are as follows:

- **Identifiability:** How easily PII can be used to identify specific individuals
- **Quantity of PII:** How many individuals are identified in the information
- **Data field sensitivity:** The sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together
- **Context of use:** The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated
- **Obligation to protect confidentiality:** The laws, regulations, standards, and operating practices that dictate an organization's responsibility for protecting PII
- **Access to and location of PII:** The nature of authorized access to PII

PII should be protected through a combination of measures, including operational safeguards, privacy-specific safeguards, and security controls. Operational safeguards should include policy and procedure creation and awareness, training, and education programs. Privacy-specific safeguards help organizations collect, maintain, use, and disseminate data in ways that protect the confidentiality of the data and include minimizing the use, collection, and retention of PII; conducting privacy impact assessments; de-identifying information; and anonymizing information. Security controls include separation of duties, least privilege, auditing, identification and authorization, and others from NIST SP 800-53.

NOTE NIST SP 800-53 is covered in more detail in Chapter 1.

Organizations that collect, use, and retain PII should use NIST SP 800-122 to help guide the organization's efforts to protect the confidentiality of PII.

PHI

Protected health information (PHI), also referred to as electronic protected health information (***EPHI*** or ePHI), is any individually identifiable health information. PHI is treated as a special case of PII with different standards and frameworks. NIST SP 800-66 provides guidelines for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The Security Rule applies to the following covered entities:

- **Covered healthcare providers:** Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which HHS (U.S. Department of Health and Human Services) has adopted a standard.
- **Health plans:** Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- **Healthcare clearinghouses:** A public or private entity that processes another entity's healthcare transactions from a standard format to a nonstandard format, or vice versa.
- **Medicare prescription drug card sponsors:** A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act.

Each covered entity must ensure the confidentiality, integrity, and availability of PHI that it creates, receives, maintains, or transmits; protect against any reasonably anticipated threats and hazards to the security or integrity of EPHI; and protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Privacy Rule.

The Security Rule is separated into six main sections as follows:

- **Security Standards General Rules:** Includes the general requirements all covered entities must meet; establishes flexibility of approach; identifies standards and implementation specifications (both required and addressable); outlines decisions a covered entity must make regarding addressable implementation specifications; and requires maintenance of security measures to continue reasonable and appropriate protection of PHI.
- **Administrative Safeguards:** Defined in the Security Rule as the "administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."
- **Physical Safeguards:** Defined as the "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
- **Technical Safeguards:** Defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."
- **Organizational Requirements:** Includes standards for business associate contracts and other arrangements, including memoranda of understanding between a covered entity and a business associate when both entities are government organizations; and requirements for group health plans.
- **Policies and Procedures and Documentation Requirements:** Requires implementation of reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule; maintenance of written documentation (which may be also in electronic form such as email) and/or records that include policies, procedures, actions, activities, or assessments required by the Security Rule; and retention, availability, and update requirements related to the documentation.

NIST SP 800-66 includes a relationship linking the NIST Risk Management Framework (RMF) and the Security Rule. It also includes key activities that should be carried out for each of the preceding six main sections of the Security Rule. Organizations that collect, use, and retain PHI should use NIST SP 800-66 to help guide the organization's efforts to provide confidentiality, integrity, and availability for PHI.

Proprietary Data

Proprietary data is defined as internally generated data or documents that contain technical or other types of information controlled by an organization to safeguard its competitive edge. Proprietary data may be protected under copyright, patent, or trade secret laws. While there are no specific and different standards or frameworks to govern the protection of proprietary data, organizations must ensure that the confidentiality, integrity, and availability of proprietary data are protected. Because of this, many organizations protect proprietary data with the same types of controls that are used for PII and PHI.

Security professionals should ensure that proprietary data is identified and properly categorized to ensure that the appropriate controls are put into place.

Private Sector Data Classifications

Organizations in the private sector can generally classify their data using four main classification levels, listed from highest sensitivity level (1) to lowest (4):

1. Confidential
2. Private
3. Sensitive
4. Public

NOTE It is up to each organization to determine the number and type of classifications. Other classification options that an organization can choose to use include "protected" to indicate legally protected data and "proprietary" to indicate company-owned data (in a legal sense).

Data that is confidential includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred. Data at this level would be available only to personnel in the organization whose work needs, or is directly related to, the accessed data.

Access to confidential data usually requires authorization for each access. In most cases, the only way for external entities to have authorized access to confidential data is as follows:

- After signing a confidentiality agreement
- When complying with a court order
- As part of a government project or contract procurement agreement

Data that is private includes any information related to personnel, including human resources records, medical records, and salary information, that is used only within the organization. Data that is sensitive includes organizational financial information and requires extra measures to ensure its CIA and accuracy. Public data is data that is generally shared with the public and would not cause a negative impact on the organization. Examples of public data include how many people work in the organization and what products an organization manufactures or sells.

Military and Government Data Classifications

Military and governmental entities usually classify data using five main classification levels, listed from highest sensitivity level to lowest:

1. **Top Secret:** Disclosure would cause exceptionally grave danger to national security.
2. **Secret:** Disclosure would cause serious damage to national security.
3. **Confidential:** Disclosure would cause damage to national security.
4. **Sensitive but Unclassified:** Disclosure might harm national security.
5. **Unclassified:** Any information that can generally be distributed to the public without any threat to national interest.

U.S. federal agencies use the Sensitive but Unclassified (SBU) designation when information is not classified but still needs to be protected and requires strict controls over its distribution. There are over 100 different labels for SBU, including

- For official use only (FOUO)
- Limited official use
- Sensitive security information
- Critical infrastructure information

Executive order 13556 created a standard designation Controlled Unclassified Information (CUI). Implementation is in progress.

Data that is top secret includes weapon blueprints, technology specifications, spy satellite information, and other military information that could gravely damage national security if disclosed. Data that is secret includes deployment plans, missile placement, and other information that could seriously damage national security if disclosed. Data that is confidential includes strength of forces in the United States and overseas, technical information used for training and maintenance, and other information that could seriously affect the government if unauthorized disclosure occurred. Data that is sensitive but unclassified includes medical or other personal data that might not cause serious damage to national security if disclosed but could cause citizens to question the reputation of the government and may even lead to legal battles with lawsuits. Military and government information that does not fall into any of the four other categories is considered unclassified and usually available to the public based on the Freedom of Information Act.

NOTE Enacted on July 4, 1966, and taking effect one year later, the Freedom of Information Act (FOIA) provides a powerful tool to advocates for access to information. Under the FOIA, anyone may request and receive any records from federal agencies unless the documents are officially declared exempt based upon specific categories, such as top secret, secret, and confidential. To learn more about how to explore for FOIA data or make a FOIA request, visit www.foia.gov.

Information and Asset Handling Requirements

Organizations should establish the appropriate information and asset handling requirements to protect their assets. As part of these handling requirements, personnel should be instructed on how to mark, label, store, and destroy or dispose of media.

Handling requirements are spelled out in organizational standards and other documentation. Organizational standards and documentations must be enforced to ensure proper asset handling. Handling requirements inform custodians and users how to protect the information they use and systems with which they interact. Handling requirements dictate by classification level how information must be stored, transmitted, communicated, accessed, retained, and destroyed. Handling requirements can extend to incident management and breach notification. Handling requirements extend to automated tools, such as data loss prevention (DLP) solutions. Handling requirements should be succinctly documented in a usable format. Handling requirements compliance should be referenced in the acceptable use policy (AUP). Users should be introduced to handling requirements during the onboarding process. Handling requirements should be reinforced throughout the user life cycle.

Marking, Labeling, and Storing

Plainly label all forms of storage media (tapes, optical drives, and so on) and store them safely. Some guidelines in the area of media control are to

- Accurately and promptly mark all data storage media.
- Ensure proper environmental storage of the media.
- Ensure the safe and clean handling of the media.
- Log data media to provide a physical inventory control.

The environment where the media will be stored is also important. For example, damage could occur to magnetic media above 100 degrees Fahrenheit (38 degrees Celsius).

Media marking refers to the use of human-readable information about the media, while *media labeling* refers to the use of security attributes in internal ***data structures***. Marking is usually written on the media itself so the correct media can be easily identified. Labeling is internal to the media itself. A backup tape may be marked with a server name or other identifier of the asset to which the backup belongs. If an administrator accesses the backups on the backup tape, each backup will be labeled with a descriptive name that usually includes the date, time, and type of backup. In addition, ACLs may be configured on the different backup files to limit the users who can access the backup files.

Labeling is the vehicle for communicating the assigned classification to custodians, users, and applications (for example, access control and DLP). Labels make it easy to identify the data classification. Labels can take many forms: electronic, print, audio, or visual. Labeling recommendations are tied to media type. In electronic form, the classification label should be a part of the document name (for example, Customer Transaction History_Protected). On written or printed documents, the classification label should be clearly watermarked, as well as in either the document header or footer. For physical media, the classification label should be clearly marked on the case using words or symbols.

Destruction

During media disposal, you must ensure no data remains on the media. The most reliable, secure means of removing data from magnetic storage media, such as a magnetic tape cassette, is through *degaussing*, which exposes the media to a powerful, alternating magnetic field. It removes any previously written data, leaving the media in a magnetically randomized (blank) state. More information on the destruction of media is given earlier in this chapter, later in the "Data Remanence and Destruction" section, and in Chapter 7, "Security Operations."

Provision Resources Securely

While information and assets within an organization are ultimately owned by the organization, it is usually understood that information and assets within the organization are owned and managed by different business units. These business units must work together to ensure that the organizational mission is achieved and that the information and assets are protected.

For this reason, security professionals must understand where the different information and assets are located and work with the various owners to ensure that the information and assets are protected. The owners that security professionals need to work with include data owners, system owners, and business/mission owners. As part of asset ownership, security professionals should ensure that appropriate asset management procedures are developed and followed, as described in Chapter 7.

Asset Inventory and Asset Management

To properly secure organizational assets, security professionals must ensure that an accurate inventory of all assets is obtained. After all assets are inventoried, assets must be managed by the asset owners. To fully understand asset inventory and management, security professionals must understand the asset life cycle. According to the National Institute of Standards (NIST), the asset life cycle is an eight-phase process, as shown in Figure 2-1.

Key Topic

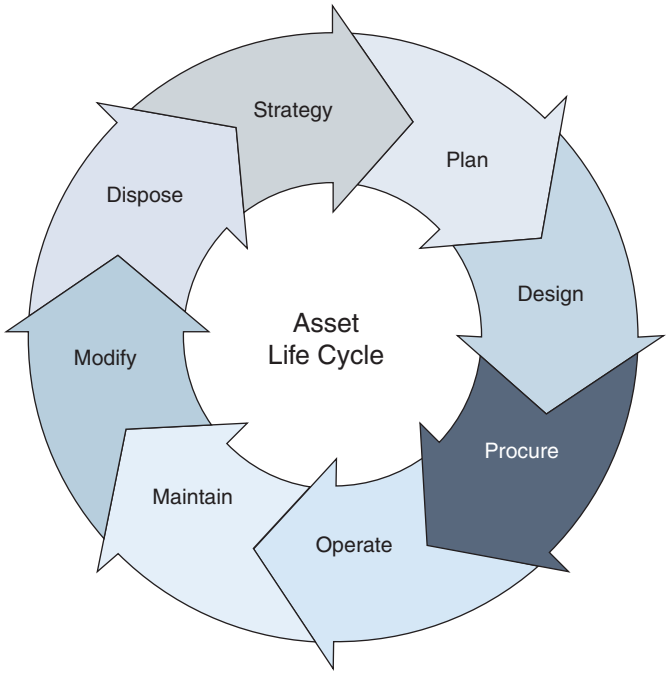

Figure 2-1 Asset Life Cycle

In a typical life cycle, an asset goes through the enrollment, operation, and end-of-life phases. The enrollment process involves manual IT staff activities, such as assigning and tagging the asset with a serial number and barcode, loading a baseline IT image, assigning the asset to an owner, and, finally, recording the serial number as well as other attributes into a database. The attributes might also include primary location, hardware model, baseline IT image, and owner. This process can also be referred to as the inventory phase.

As the asset goes through the operations phase, changes can occur. Such changes could include introduction of new or unauthorized software, the removal of certain critical software, or the removal of the physical asset itself from the enterprise. These changes need to be tracked and recorded. As a consequence, asset monitoring, anomaly detection, reporting, and policy enforcement are the primary activities in this phase.

The assets within the enterprise are monitored using installed agents that reside on the asset, as well as network-based monitoring systems that scan and capture network traffic. These monitoring systems collect data from and about the assets and send periodic reports to the analytics engine.

As an asset reaches the end of its operational life, it goes through activities within the end-of-life phase that include returning the asset to IT support for data removal and removing the serial number (or other organization labeling information) from the registration database and other associated databases. Finally, the asset is prepared for physical removal from the enterprise facility.

Asset management includes the operate, maintain, and modify phases of the asset life cycle. After an asset is configured as it should be with all updates and settings, administrators should document the configuration baseline, which is a description of an asset's attributes at a point in time, which serves as a basis for defining change. (Configuration and change management are discussed in more detail in Chapter 7.) As part of asset management, an asset's security and configuration baseline should be enforced by configuration management agents, and installed software is captured by software asset management agents. Both categories of agents forward reports to their respective servers, which serve as data storage facilities. Reports can be compiled based on the data received from the agents and sent to those responsible for managing the assets. Regular examination of these reports should be a priority to ensure that assets have the appropriate security controls.

Data Life Cycle

A *data life cycle* refers to the entire period of time that an organization retains data. The following sections discuss the data life cycle, databases, roles and

responsibilities, data collection and limitation, data location, data maintenance, data retention, data remanence and destruction, and data audit.

Organizations should ensure that any information they collect and store is managed throughout the life cycle of that information. If no information life cycle is followed, the data would be retained indefinitely, never discarded, and rarely, if ever, updated. Security professionals must therefore ensure that data owners and custodians understand the information life cycle.

For most organizations, the five phases of the information life cycle are as follows:

1. Create/receive
2. Distribute
3. Use
4. Maintain
5. Dispose/store

During the create/receive phase, data is either created by organizational personnel or received by the organization via the data entry portal. If the data is created by organizational personnel, it is usually placed in the location from which it will be distributed, used, and maintained. However, if the data is received via some other mechanism, you might need to copy or import the data to an appropriate location. In this case, the data will not be available for distribution, usage, and maintenance until after the copy or import. Not all data is used by all users. As such, data needs to be sorted, stored, and distributed in various ways as the needs arise from each user or business unit. This phase also must contain data classification after receiving and creating. Received or created data must be given a classification and sensitivity before it can be distributed or data will be going everywhere.

After the create/receive phase, organizational personnel must ensure that the data is properly distributed. In most cases, this step involves placing the data in the appropriate location and possibly configuring the access permissions as defined by the data owner. Keep in mind, however, that in many cases the storage location and appropriate user and group permissions may already be configured. In such a case, it is just a matter of ensuring that the data is in the correct distribution location. Distribution locations include databases, shared folders, ***network-attached storage (NAS)***, storage-area networks (SANs), and data libraries.

After data has been distributed, personnel within the organization can use the data in their day-to-day operations. Whereas some personnel will have only read access to data, others may have write or full control permissions. Remember that the

permissions allowed or denied are designated by the data owner but configured by the data custodian.

Now that data is being used in day-to-day operations, data maintenance is key to ensuring that data remains accessible and secure. Maintenance includes auditing, performing backups, performing data integrity checks, and managing data leaks and loss.

When data becomes old, invalid, and not fit for any further use, it is considered to be in the disposition stage. You should either properly dispose of it or ensure that it is securely stored. Some organizations must maintain data records for a certain number of years per local, state, or federal laws or regulations. This type of data should be archived for the required period. In addition, any data that is part of litigation should be retained as requested by the court of law, and organizations should follow appropriate chain of custody and evidence documentation processes. Data archival and destruction procedures should be clearly defined by the organization.

All organizations need policies in place for the retention and destruction of data. Data retention and destruction must follow all local, state, and government regulations and laws. Documenting proper procedures ensures that information is maintained for the required time to prevent financial fines and possible incarceration of high-level organizational officers. These procedures must include both the retention period and destruction process.

Figure 2-2 shows the information life cycle.

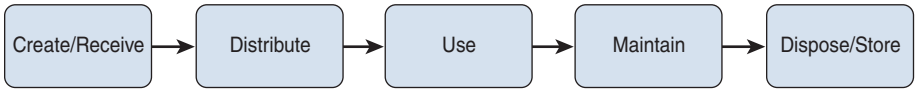

Figure 2-2 Information Life Cycle

A discussion of data would be incomplete without a discussion of databases.

Databases

Databases have become the technology of choice for storing, organizing, and analyzing large sets of data. End users who use data from databases generally access a database though a client interface. As the need arises to provide access to entities outside the enterprise, the opportunities for misuse increase. In the following sections, concepts necessary to discuss database security are covered as well as the security concerns surrounding database management and maintenance.

DBMS Architecture and Models

Databases contain data, and the main difference in database models is how that information is stored and organized. The model describes the relationships among the data elements, how the data is accessed, how integrity is ensured, and acceptable operations. The five models or architectures we discuss are

- Relational
- Hierarchical
- Network
- Object-oriented
- Object-relational

The *relational* model uses *attributes* (columns) and *tuples* (rows) to organize the data in two-dimensional tables. Each cell in the table represents the intersection of an attribute, and a tuple represents a record.

When working with relational database management systems (RDBMSs), you should understand the following terms:

- ***Relation*:** A connection between one or more tables. One column in a table is a primary key that relates to another table as a foreign key.
- **Tuple:** A ***row*** in a table.
- **Attribute:** A column in a table.
- ***Schema*:** Description of a ***relational database***.
- ***Record*:** A collection of related data items.
- ***Base relation*:** In SQL, a relation that is actually existent in the database.
- ***View*:** The set of data derived from one or more tables or views available to a given user. Security is enforced through the use of views for users needing read-only access to the data.
- ***Degree*:** The number of columns in a table.
- ***Cardinality*:** The number of rows in a relation.
- ***Domain*:** The set of allowable values that an attribute can take.
- **Primary key:** One or more columns that identify each row of a table unique.
- ***Foreign key*:** An attribute in one relation that has values matching the primary key in another relation. Matches between the foreign key and the primary key

are important because they represent references from one relation to another and establish the connection among these relations.

- ***Candidate key*:** An attribute in a row that uniquely identifies that row.
- ***Referential integrity*:** A requirement that for any foreign key attribute, the referenced relation must have a tuple with the same value for its primary key.

An important element of database design that ensures that the attributes in a table depend only on the primary key is a process called *normalization*. Normalization includes

- Eliminating repeating groups by putting them into separate tables
- Eliminating redundant data (occurring in more than one table)
- Eliminating attributes in a table that are not dependent on the primary key of that table

In the ***hierarchical database*** model, data is organized into a hierarchy. An object can have one child (an object that is a subset of the parent object), multiple children, or no children. To navigate this hierarchy, you must know the branch in which the object is located. An example of the use of this system is the Windows Registry and a Lightweight Directory Access Protocol (LDAP) directory.

In the *network* model, as in the hierarchical model, data is organized into a hierarchy, but unlike the hierarchical model, objects can have multiple parents. Because of this, knowing which branch to find a data element in is not necessary because there will typically be multiple paths to it.

The *object-oriented* model can handle a variety of data types and is more dynamic than a relational database. ***Object-oriented database (OODB)*** systems are useful in storing and manipulating complex data, such as images and graphics. Consequently, complex applications involving multimedia, computer-aided design (CAD), video, graphics, and expert systems are more suited to the object-oriented model. It also has the characteristics of ease of reusing code and analysis and reduced maintenance.

Objects can be created as needed, and the data and the procedures (or methods) go with the object when it is requested. A *method* is the code defining the actions that the object performs in response to a message. This model uses some of the same concepts of a relational model. In the object-oriented model, the relation, column, and tuple (relational terms) are referred to as class, attribute, and instance objects.

The *object-relational* model is the marriage of object-oriented and relational technologies, combining the attributes of both. This is a relational database with a software interface that is written in an ***object-oriented programming (OOP)*** language. The

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

U

V

W

X

Y-Z