EXAM CRAM

CISSP®

Fourth Edition

PEARSON IT
CERTIFICATION

MICHAEL GREGG

EXAM CRAM

CISSP® Exam Cram

Fourth Edition

Michael Gregg

CISSP® Exam Cram, Fourth Edition

ISBN-13: 978-0-7897-5553-7

ISBN-10: 0-7897-5553-X

Library of Congress Control Number: 2016940474

Printed in the United States of America

First Printing: August 2016

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Michelle Newcomb

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Larry Sulky

Indexer
Lisa Stumpf

Proofreader
H.S. Rupa

Technical Editors
Chris Crayton
Michael Angelo

Publishing Coordinator
Vanessa Evans

Page Layout
codeMantra

Contents at a Glance

Table of Contents

About the Author

As the CEO of Superior Solutions, Inc., a Houston-based IT security consulting and auditing firm, **Michael Gregg** has more than 20 years of experience in information security and risk management. He holds two associate's degrees, a bachelor's degree, and a master's degree. Some of the certifications he holds include CISSP, SSCP, MCSE, CTT+, A+, N+, Security+, CASP, CCNA, GSEC, CEH, CHFI, CEI, CISA, CISM, and CGEIT.

In addition to his experience with performing security audits and assessments, Gregg has authored or coauthored more than 20 books, including *Certified Ethical Hacker Exam Prep* (Que), *CISSP Exam Cram 2* (Que), and *Security Administrator Street Smarts* (Sybex). He has testified before U.S. Congress, his articles have been published on IT websites, and he has been sourced as an industry expert for CBS, ABC, CNN, Fox News and the New York Times. He has created more than 15 security-related courses and training classes for various companies and universities. Although audits and assessments are where he spends the bulk of his time, teaching and contributing to the written body of IT security knowledge are how Michael believes he can give something back to the community that has given him so much.

He is a board member for Habitat for Humanity and when not working, Michael enjoys traveling and restoring muscle cars.

About the Technical Reviewers

Chris Crayton (MCSE) is an author, technical consultant, and trainer. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

Michael Angelo During his tenure in security he was responsible for the secure development, implementation, and deployment of products. This included driving the creation of security solutions, policies and procedures, threat modeling and product analysis exercises, practical encryption techniques, biometric and token access authentication technology, common criteria certifications, and residual risk management scoring methodologies.

Amongst his accomplishments, Michael has 57 U.S. patents, was recognized by the City of Houston as the "2003 Inventor of the Year," and is a former Sigma-Xi distinguished lecturer. In 2011, he was named ISSA Security Professional of the Year and in 2013 was added to the ISSA Hall of Fame.

Dedication

I dedicate this book to my godson, Alexander Bucio.
May his life be filled with success and happiness. Mucho gusto!

Acknowledgments

I would like to thank my wife, Christine, for understanding the long hours such a project entails. Also, thanks to Michelle Newcomb and the entire Pearson crew.

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: feedback@pearsonitcertification.com
Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *CISSP Exam Cram* 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 9780789755537 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.

This page intentionally left blank

Introduction

Welcome to *CISSP® Exam Cram!* This book covers the CISSP certification exam. Whether this is your first or your fifteenth *Exam Cram*, you'll find information here and in Chapter 1 that will ensure your success as you pursue knowledge, experience, and certification. This introduction explains the ISC^2 certification programs in general and talks about how the *Exam Cram* series can help you prepare for the CISSP exam.

This book is one of the *Exam Cram* series of books and will help by getting you on your way to becoming an ISC^2 Certified Information Systems Security Professional (CISSP).

This introduction discusses the basics of the CISSP exam. Included are sections covering preparation, how to take an exam, a description of this book's contents, how this book is organized, and, finally, author contact information.

Each chapter in this book contains practice questions. There are also two full-length practice exams at the end of the book. Practice exams in this book should provide an accurate assessment of the level of expertise you need to obtain to pass the test. Answers and explanations are included for all test questions. It is best to obtain a level of understanding equivalent to a consistent pass rate of at least 95% on the practice questions and exams in this book before you attempt the real exam.

Let's begin by looking at preparation for the exam.

How to Prepare for the Exam

Preparing for the CISSP exam requires that you obtain and study materials designed to provide comprehensive information about security. The following list of materials will help you study and prepare:

- The ISC^2 website at www.isc2.org
- The exam outline available at the ISC^2 website

Many people form study groups, attend seminars, and attend training classes to help them study for and master the material needed to pass the CISSP exam.

Practice Tests

You don't need to know much about practice tests, other than that they are a worthwhile expense for three reasons:

- They help you diagnose areas of weakness.
- They are useful for getting used to the format of questions.
- They help you to decide when you are ready to take the exam.

This book contains questions at the end of each chapter and includes two full-length practice tests. However, if you still want more, a related *Exam Cram CISSP Practice Questions* book has more than 500 additional questions. Many other companies provide CISSP certification practice tests, flash cards, and aids as well.

Taking a Certification Exam

When you have prepared for the exam, you must register with ISC^2 to take the exam. The CISSP exam is given at Pearson VUE testing centers. ISC^2 has implemented regional pricing: As an example, as of the publication of this book registration is $599 in the United States. Check the Pearson VUE website at www.pearsonvue.com to get specific details.

After you register, you will receive a confirmation notice. Some locations may have limited test centers available, which means that you should schedule your exam in advance to make sure you can get the specific date and time you would like.

Arriving at the Exam Location

As with any examination, arrive at the testing center early. Be prepared! You will need to bring the confirmation letter and identification, such as a driver's license, green card, or passport. Any photo ID will suffice. Two forms of ID are usually required. The testing center staff requires proof that you are who you say you are and that someone else is not taking the test for you. Arrive early because if you are late, you will be barred from entry and will not receive a refund for the cost of the exam.

ExamAlert

You'll be spending a lot of time in the exam room. The total test time is six hours, so eat a good breakfast. Policies differ from location to location regarding bathroom breaks—check with the testing center before beginning the exam.

In the Testing Center

You will not be allowed to take study materials or anything else into the examination room with you that could raise suspicion that you're cheating. This includes practice test material, books, exam prep guides, or other test aids.

After the Exam

Examination results are available after the exam. If you pass the exam, you will simply receive a passing grade—your exact score will not be provided. Candidates who do not pass will receive a complete breakdown on their score by domain. This allows those individuals to see what areas they are weak in.

Retaking a Test

If you fail the exam, you must wait at least 30 days to take it again. Each of the ten domains will be shown, with your score in each. As an example, you may have received a 95% score in the Communications and Network Security domain and only 12% in Asset Security. Use this feedback to better understand what areas you were weak in and where to spend your time and effort in your studies. Additionally, invest in some practice tests if you have not already done so. There is much to be said for getting used to a testing format.

Tracking Your CISSP Status

When you pass the exam, you still need to attest to the CISSP code of ethics and have an existing CISSP complete an endorsement form for you.

When you pass the exam, you will next be required to complete an endorsement form. The endorsement form must be completed by someone who can attest to your professional experience and who is an active CISSP in good standing. If you don't know anyone who is CISSP-certified, ISC^2 allows endorsements from other professionals who are certified, licensed, or

commissioned, and an officer of the corporation where you are employed. You can review complete information on the endorsement form at the ISC^2 website.

About This Book

The ideal reader for an *Exam Cram* book is someone seeking certification. However, it should be noted that an *Exam Cram* book is an easily readable, rapid presentation of facts. Therefore, an *Exam Cram* book is also extremely useful as a quick reference manual.

Most people seeking certification use multiple sources of information. Check out the links at the end of each chapter to get more information about subjects you're weak in. Various security books from retailers also describe the topics in this book in much greater detail. Don't forget that many have described the CISSP exam as being a "mile wide."

This book includes other helpful elements in addition to the actual logical, step-by-step learning progression of the chapters themselves. *Exam Cram* books use elements such as exam alerts, tips, notes, and practice questions to make information easier to read and absorb.

> **Note**
>
> Reading this book from start to finish is not necessary; this book is set up so that you can quickly jump back and forth to find sections you need to study.

Use the *Cram Sheet* to remember last-minute facts immediately before the exam. Use the practice questions to test your knowledge. You can always brush up on specific topics in detail by referring to the table of contents and the index. Even after you achieve certification, you can use this book as a rapid-access reference manual.

The Chapter Elements

Each *Exam Cram* book has chapters that follow a predefined structure. This structure makes *Exam Cram* books easy to read and provides a familiar format for all *Exam Cram* books. The following elements typically are used:

- Opening hotlists
- Chapter topics

- Exam Alerts
- Notes
- Tips
- Sidebars
- Cautions
- Exam preparation practice questions and answers
- A "Need to Know More?" section at the end of each chapter

Note

Bulleted lists, numbered lists, tables, and graphics are also used where appropriate. A picture can paint a thousand words sometimes, and tables can help to associate different elements with each other visually.

Now let's look at each of the elements in detail.

- **Opening hotlists**—The start of every chapter contains a list of terms you should understand. A second hotlist identifies all the techniques and skills covered in the chapter.
- **Chapter topics**—Each chapter contains details of all subject matter listed in the table of contents for that particular chapter. The objective of an *Exam Cram* book is to cover all the important facts without giving too much detail; it is an exam cram. When examples are required, they are included.
- **Exam Alerts**—Exam Alerts address exam-specific, exam-related information. An Exam Alert addresses content that is particularly important, tricky, or likely to appear on the exam. An Exam Alert looks like this:

ExamAlert

Make sure you remember the different ways in which DES can be implemented and that ECB is considered the weakest form of DES.

- **Notes**—Notes typically contain useful information that is not directly related to the current topic under consideration. To avoid breaking up the flow of the text, they are set off from the regular text.

Note

This is a note. You have already seen several notes.

- **Tips**—Tips often provide shortcuts or better ways to do things.

Tip

A clipping level is the point at which you set a control to distinguish between activity that should be investigated and activity that should not be investigated.

- **Sidebars**—Sidebars are longer and run beside the text. They often describe real-world examples or situations.

How Caller ID Can Be Hacked

Sure, we all trust caller ID, but some Voice over IP (VoIP) providers allow users to inject their own call party number (CPN) into the call. Because VoIP is currently outside FCC regulation, these hacks are now possible.

- **Cautions**—Cautions apply directly to the use of the technology being discussed in the Exam Cram. For example, a Caution might point out that the CER is one of the most important items to examine when examining biometric devices.

Caution

The crossover error rate (CER) is the point at which Type 1 errors and Type 2 errors intersect. The lower the CER is, the more accurate the device is.

- **Exam preparation practice questions**—At the end of every chapter is a list of at least 10 exam practice questions similar to those in the actual exam. Each chapter contains a list of questions relevant to that chapter, including answers and explanations. Test your skills as you read.
- **"Need to Know More?" section**—This section at the end of each chapter describes other relevant sources of information. With respect to this chapter, the best place to look for CISSP certification information is at the ISC^2 website, www.ISC2.org.

Other Book Elements

Most of this *Exam Cram* book on CISSP follows the consistent chapter structure already described. However, there are various, important elements that are not part of the standard chapter format. These elements apply to the entire book as a whole.

- **Practice exams**—In addition to exam-preparation questions at the end of each chapter, two full practice exams are included at the end of the book.
- **Answers and explanations for practice exams**—These follow each practice exam, providing answers and explanations to the questions in the exams.
- **Glossary**—The glossary contains a listing of important terms used in this book with explanations.
- **Cram Sheet**—The Cram Sheet is a quick-reference, tear-out cardboard sheet of important facts useful for last-minute preparation. Cram Sheets often include a simple summary of facts that are most difficult to remember.
- **Companion website**—The companion website contains the Pearson IT Certification Practice Test engine, which provides multiple test modes that you can use for exam preparation. The practice tests are designed to appropriately balance the questions over each technical area (domain) covered by the exam. All concepts from the actual exam are covered thoroughly to ensure you're prepared for the exam.

Chapter Contents

The following list provides an overview of the chapters.

- **Chapter 1, "The CISSP Certification Exam"**—This chapter introduces exam strategies and considerations.
- **Chapter 2, "Logical Asset Security"**—This chapter discusses logical security and the countermeasures available for protecting an organization's resources. Key topics include CIA, data classification, and control of an organization's assets from creation to destruction.
- **Chapter 3, "Physical Asset Security"**—This chapter discusses physical security and the importance of providing physical protection for an organization's resources. Physical security plays a key role in securing an organization's assets. Without effective physical security, there can be no effective security structure at all.

- **Chapter 4, "Security and Risk Management"**—This chapter discusses asset management and the protection of critical resources. Quantitative and qualitative risk assessment are two major topics of this chapter. Readers must understand how these concepts are used to assess and measure risk while reducing threats to the organization. Key concepts include the development of policies, procedures, guidelines, and assorted controls.
- **Chapter 5, "Security Engineering"**—This chapter discusses key concepts such as computer hardware, operating system design, security models (Biba, Bell-LaPadula, Clark-Wilson, etc.) and documentation used to verify, certify, and accredit systems and networks.
- **Chapter 6, "The Application and Use of Cryptography"**—This chapter discusses the methods and systems used to encrypt and protect data. Symmetric, asymmetric, and hashing algorithms are introduced, along with PKI and cryptographic methods of attack.
- **Chapter 7, "Communication and Network Security"**—This chapter discusses telecommunication technology. Items such as the OSI model, TCP/IP, network equipment, LAN, MAN, and WAN protocols, and wireless technologies are just a few of the technologies discussed. This is an expansive domain and covers a lot of information for the CISSP candidate to master.
- **Chapter 8, "Identity and Access Management"**—This chapter covers the basics of access control. It addresses the three A's: authentication, authorization, and accountability. Items like identification, single sign-on, centralized authentication, and federation are discussed.
- **Chapter 9, "Security Assessment and Testing"**—This chapter discusses security assessments, ethical hacking, and vulnerability scanning. It also reviews common types of malware and various attack methodologies.
- **Chapter 10, "Security Operations"**—This chapter covers operation controls—that is, the types of controls that the organization can implement. Topics such as background checks, dual controls, mandatory vacations, rotation of duties, and auditing are introduced.
- **Chapter 11, "Software Development Security"**—This chapter discusses databases, the system development life cycle, and the importance of building security into applications and systems as early as possible during the development process. Project management is reviewed, as are malicious code, knowledge-based systems, and application issues.

- **Chapter 12, "Business Continuity Planning"**—This chapter covers all the aspects of the BCP process. Although some may discount the importance of this domain, storms, floods, hurricanes, earthquakes, and other natural disasters. should demonstrate the criticality of this domain. This chapter addresses key elements of disaster recovery. One important item is that no demonstrated recovery exists until the business continuity plan has been tested. Exam candidates must understand what is needed to prevent, minimize, and recover from disasters.
- **Practice Exam I**—This is a full-length practice exam.
- **Answers to Practice Exam I**—This element contains the answers and explanations for the first practice exam.
- **Practice Exam II**—This is a second full-length practice exam.
- **Answers to Practice Exam II**—This element contains the answers and explanations for the second practice exam.

Companion Website

Register this book to get access to the Pearson IT Certification test engine and other study materials, plus 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 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 the steps below:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: 9780789757142.
3. Answer the challenge question as proof of purchase.
4. Click on 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 at left, please visit www.pearsonITcertification.com/contact and select the "Site Problems/Comments" option. Our customer service representatives will assist you.

Pearson IT Certification Practice Test Engine and Questions

The companion site includes the Pearson IT Certification Practice Test engine—software that displays and grades a set of exam-realistic multiple-choice questions. Using the Pearson IT Certification Practice Test engine, you can either study by going through the questions in Study Mode, or take a simulated exam that mimics real exam conditions.

The installation process requires two major steps: installing the software and then activating the exam. The website has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on this site.

> **Note**
>
> The cardboard case in the back of this book includes a piece of paper. The paper lists the activation code for the practice exam associated with this book. Do not lose the activation code. Also included on the paper is a unique, one-time use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Install the Software

The Pearson IT Certification Practice Test is a Windows-only desktop application. You can run it on a Mac using a Windows Virtual Machine, but it was built specifically for the Windows platform. The minimum system requirements are:

- Windows 10, Windows 8.1, or Windows 7
- Microsoft .NET Framework 4.5 Client
- Pentium class 1 GHz processor (or equivalent)
- 512 MB RAM

- 650 MB disc space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

The software installation process is pretty routine compared to other software installation processes. If you have already installed the Pearson IT Certification Practice Test software from another Pearson product, there is no need for you to reinstall the software. Simply launch the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in the access code card sleeve in the back of the book.

The following steps outline the installation process:

1. Download the exam practice test engine from the companion site.
2. Respond to Windows prompts as with any typical software installation process.

The installation process will give you the option to activate your exam with the activation code supplied on the paper in the cardboard sleeve. This process requires that you establish a Pearson website login. You will need this login in order to activate the exam, so please do register when prompted. If you already have a Pearson website login, there is no need to register again. Just use your existing login.

Activate and Download the Practice Exam

Once the exam engine is installed, you should then activate the exam associated with this book (if you did not do so during the installation process), as follows:

Step 1: Start the Pearson IT Certification Practice Test software from the Windows **Start** menu or from your desktop shortcut icon.

Step 2: To activate and download the exam associated with this book, from the **My Products** or **Tools** tab, select the **Activate** button.

Step 3: At the next screen, enter the activation code from the paper inside the cardboard holder in the back of the book. Once entered, click the **Activate** button.

Step 4: The activation process will download the practice exam. Click **Next**, and then click **Finish**.

Once the activation process is completed, the **My Products** tab should list your new exam. If you do not see the exam, make sure you have selected the **My Products** tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Open Exam** button.

To update a particular exam that you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Updating your exams will ensure you have the latest changes and updates to the exam data.

If you wish to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab and select the **Update Application** button. This will ensure you are running the latest version of the software engine.

Activating Other Exams

The exam software installation process, and the registration process, only has to happen once. Then, for each new exam, only a few steps are required. For instance, if you buy another new Pearson IT Certification book, extract the activation code from the cardboard sleeve in the back of that book—you don't even need the exam engine at this point. From there, all you have to do is start the exam engine (if not still up and running), and perform steps 2 through 4 from the previous list.

Contacting the Author

Hopefully, this book provides you with the tools you need to pass the CISSP exam. Feedback is appreciated. You can contact the author at mikeg@thesolutionfirm.com.

Thank you for selecting my book; I have worked to apply the same concepts in this book that I have used in the hundreds of training classes I have taught. Spend your study time wisely and you, too, can become a CISSP. Good luck on the exam!

Self-Assessment

This self-assessment section enables you to evaluate your readiness to take the CISSP certification exam. It should also help you understand what's required to obtain the CISSP certification. Are you ready?

CISSPs in the Real World

Security continues to be on everyone's mind. The CISSP certification continues to be one of the most sought-after security certifications. Increasing numbers of people are studying for and obtaining their CISSP certifications. Congratulations on making the decision to follow in their footsteps. If you are willing to tackle the process seriously and do what it takes to obtain the necessary experience and knowledge, you can pass the exam on the first try.

> **Tip**
>
> You can also assess your CISSP skill set by using the MeasureUp Certification Mode.

The Ideal CISSP Candidate

The CISSP is designed for individuals who are leading, planning, organizing, or controlling the security initiative of an organization. The ideal CISSP candidate is likely to have a 4-year college education and have at least 5–7 years' experience in one or more of the 8 CISSP domains. The most applicable degree is in computer science or perhaps a related field. A degree is not a prerequisite for taking the test. However, exam candidates must have a minimum of 5 years of direct full-time security work experience in 2 or more of the 8 domains. One year of experience can be substituted for a 4-year college degree or an approved certification such as CompTIA Security+ or CASP. The complete list of approved certifications can be found at www.isc2.org/credential_waiver/default.aspx

Don't be lulled into thinking that this is an easy test. Some words of caution might be in order:

- The CISSP exam requires the candidate to absorb a substantial amount of material. The test is 6 hours long and consists of 225 graded questions. This is longer than typical exams at Microsoft and most other IT vendors.
- The pass mark is set high, at 700 points. The individual questions are weighted, which means that harder questions are worth more than easier ones.
- Most of the individuals attempting the exam are familiar with one to three of the domains. This means that studying for the exam can be

overwhelming because there is so much material to cover. This book can help by guiding you to the areas in which you are weak or strong.

- To be eligible for the CISSP exam, students are required to have five years of experience, or four years of experience and a college degree.

Put Yourself to the Test

In this section, you answer some simple questions. The objective is for you to understand exactly how much work and effort you must invest to pass the CISSP certification exam. The simple answer to this question is this: The experience and education you have will dictate how difficult it will be for you to pass. Be honest in your answers or you will end up wasting around $600 on an exam you were not ready to take. From the beginning, two things should be clear:

- Any educational background in computer science will be helpful, as will other IT certifications you have achieved.
- Hands-on actual experience is not only essential, but also required to obtain this certification.

Your Educational Background

- **Do you have a computer science degree?**

  You'll have a good basic knowledge needed for three or more of the eight domains, assuming that you finished your degree and your schooling and have some fairly sophisticated computer skills. Subject areas such as application development, networking, and database design are a great help.

- **Did you attend some type of technical school or week-long CISSP course?**

  This question applies to low-level or short-term computer courses. Many of these courses are extremely basic or focused in one particular area. Although the CISSP exam is not platform-specific, training classes that focused on networking, security, hacking, or database design will help you pass the exam.

- **Have you developed any security policies, performed security audits, performed penetration tests, or developed response plans?**

  If yes, you will probably be able to handle about half of the CISSP exam domains.

- **Do you have a photographic memory?**

  If yes, you might have a slim chance of passing simply by reading this book, taking some practice exams, and using the Internet to brush up on the subjects you are weak in. However, the goal here is to gain a real understanding of the material. As a CISSP, you might be asked to lead, plan, organize, or control your organization's security operations; if that happens, you'll need a real understanding of how the various technologies and techniques work. Don't cheat yourself or gamble with your career.

Again, the education and requirements given here are by no means absolute. Still, an education can give you a very good grounding in any endeavor—the higher the level of education, the better.

Testing Your Exam Readiness

Whether you attend a training class, form a study group, or study on your own, preparing for the CISSP exam is essential. The exam will cost you about $600, depending on where you are located, so you'll want to do everything you can to make sure you pass on the first try. Reading, studying, and taking practice exams are the best ways to increase your readiness. Practice exams help in two main ways:

- Practice exams highlight weak spots for further study.
- Practice exams give you a general perspective on the question format. Practicing the questions the way they are asked can help enormously on the actual testing day.

Two full-length practice exams are provided with this book. Que also publishes a second book, CISSP Practice Questions Exam, with more than 500 practice CISSP test questions; it is an excellent supplement to this book.

After the Exam

After you have passed the exam, you will need to gain continuing education credits each year to maintain your certification. Your certification will come up for renewal every 3 years, so you'll need to obtain 120 continuing education credits (CPE) or retake the exam. Retaking the exam is not a popular choice. These are some ways to gain CPEs to keep your certification current:

- Write a book.
- Read a book. (Only one per year can be used for credit.) This will give you a couple of credits, but not enough to keep your certification current.

- Do volunteer work that is approved by ISC^2. When you are certified, you can log on to the ISC^2 website for more information. A variety of volunteer work is available.
- Attend a training class. Just about any type of technology training class is accepted as long as it is tied to one of the domains.
- Teach a training class.
- Attend a college-level security class.

As you can see, the goal here is to help you stay current. As technology changes, we all must continue to learn to keep up the pace.

Now that we have covered some of the ways in which to assess your exam readiness, let's move on to Chapter 1, "The CISSP Certification Exam," where you will learn more about how the exam is structured and some effective test-taking strategies.

CHAPTER 2

Logical Asset Security

Terms you'll need to understand:

- Confidentiality
- Integrity
- Availability
- SANs
- Information lifecycle management
- Privacy impact assessment
- Data classification
- Data destruction
- Data remanence

Techniques you'll need to master:

- Proper methods for destruction of data
- Development of documents that can aid in compliance of all local, state, and federal laws
- The implementation of encryption and its use for the protection of data
- International concerns of data management

Introduction

Asset security addresses the controls needed to protect data throughout its lifecycle. From the point of creation to the end of its life, data protection controls must be implemented to ensure that information is adequately protected during each life cycle phase. This chapter starts by reviewing the basic security principles of confidentiality, integrity, and availability and moves on to data management and governance.

A CISSP must know the importance of data security and how to protect it while it is in transit, in storage, and at rest. A CISSP must understand that protection of data is much more important today than it was ten to fifteen years ago because data is no longer in just a paper form. Today, data can be found on local systems, RAID arrays, or even in the cloud. Regardless of where the data is stored it must have adequate protection and be properly disposed of at the end of its useful life.

Basic Security Principles

Confidentiality, integrity, and availability (CIA) define the basic building blocks of any good security program when defining the goals for network, asset, information, and/or information system security and are commonly referred to collectively as the CIA triad. Although the abbreviation CIA might not be as intriguing as the United States government's spy organization, it is a concept that security professionals must know and understand.

Confidentiality addresses the secrecy and privacy of information and preventing unauthorized persons from viewing sensitive information. There are a number of controls used in the real world to protect the confidentiality of information, such as locked doors, armed guards, and fences. Administrative controls that can enhance confidentiality include the use of information classification systems, such as requiring sensitive data be encrypted. For example, news reports have detailed several large-scale breaches in confidentiality as a result of corporations misplacing or losing laptops, data, and even backup media containing customer account, name, and credit information. The simple act of encrypting this data could have prevented or mitigated the damage. Sending information in an encrypted format denies attackers the opportunity to intercept and sniff clear text information.

Integrity is the second leg in the security triad. Integrity provides accuracy of information, and offers users a higher degree of confidence that the information they are viewing has not been tampered with. Integrity must be protected while in storage, at rest, and in transit. Information in storage can be protected by using access controls and audit controls. Cryptography can enhance this protection through the use of hashing algorithms. Real-life examples of this technology can be seen in programs such as Tripwire, and MD5Sum. Likewise, integrity in transit can be ensured primarily by the use of transport protocols, such as PKI, hashing, and digital signatures.

The concept of *availability* requires that information and systems be available when needed. Although many people think of availability only in electronic terms, availability also applies to physical access. If, at 2 a.m., you need access to backup media stored in a facility that allows access only from 8 a.m. to 5 p.m., you definitely have an availability problem. Availability in the world of electronics can manifest itself in many ways. Access to a backup facility 24×7 does little good if there are no updated backups to restore from.

Backups are the simplest way to ensure availability. Backups provide a copy of critical information, should data be destroyed or equipment fail. Failover equipment is another way to ensure availability. Systems such as redundant arrays of independent disks (RAID) and redundant sites (hot, cold, and warm) are two other examples. Disaster recovery is tied closely to availability because it's all about getting critical systems up and running quickly.

Which link in the security triad is considered most important? That depends. In different organizations with different priorities, one link might take the lead over the other two. For example, your local bank might consider integrity the most important; however, an organization responsible for data processing might see availability as the primary concern, whereas an organization such as the NSA might value confidentiality the most. Finally, you should be comfortable seeing the triad in any form. Even though this book refers to it as CIA, others might refer to it as AIC, or as CAIN (where the "N" stands for *nonrepudiation)*.

Security management does not stop at CIA. These are but three of the core techniques that apply to asset security. True security requires defense-in-depth. In reality, many techniques are required to protect the assets of an organization; take a moment to look over Figure 2.1.

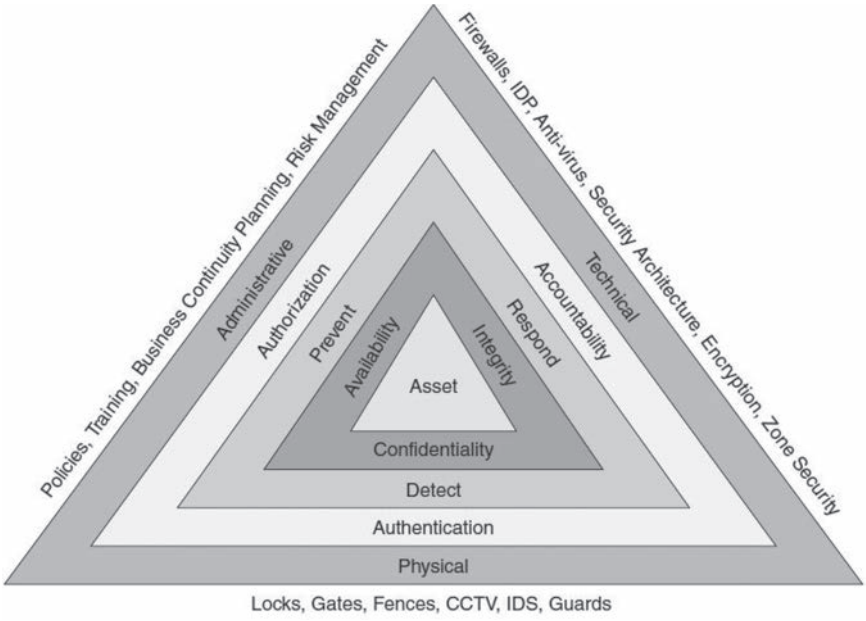

FIGURE 2.1 **Asset protection triad.**

Data Management: Determine and Maintain Ownership

Data management is not easy and has only become more complex over the last ten to fifteen years. Years ago, people only had to be concerned with paper documents and control might have only meant locking a file cabinet. Today, electronic data might be found on thumb drives, SAN storage arrays, laptop hard drives, mobile devices, or might even be stored in a public cloud.

Data Governance Policy

Generally you can think of policies as high-level documents developed by management to transmit the guiding strategy and philosophy of management to employees. A data governance policy is a documented set of specifications for the guarantee of approved management and control of an organization's digital assets and information. Data governance programs generally address the following types of data:

- Sets of master data
- Metadata

- Sensitive data
- Acquired data

Such specifications can involve directives for business process management (BPM) and enterprise risk planning (ERP), as well as security, data quality, and privacy. The goal of data governance is:

- To establish appropriate responsibility for the management of data
- To improve ease of access to data
- To ensure that once data are located, users have enough information about the data to interpret them correctly and consistently
- To improve the security of data, including confidentiality, integrity, and availability

Issues to consider include:

- **Cost**—This can include the cost of providing access to the data as well as the cost to protect it.
- **Ownership**—This includes concerns as to who owns the data or who might be a custodian. As an example, you may be the custodian of fifty copies of Microsoft Windows Server 2012 yet the code is owned by Microsoft. This is why users pay for a software license and not the ownership of the software itself, and typically have only the compiled ".exe" file and not the source code itself.
- **Liability**—This refers to the financial and legal costs an organization would bear should data be lost, stolen, or hacked.
- **Sensitivity**—This includes issues related to the sensitivity of data that should be protected against unwarranted disclosure. As an example, social security numbers, data of birth, medical history, etc.
- **Ensuring Law/Legal Compliance**—This includes items related to legal compliance. As examples, you must retain tax records for a minimum number of years, while you may only retain customers' for only the time it takes to process a single transaction.
- **Process**—This includes methods and tools used to transmit or modify the data.

Roles and Responsibility

Data security requires responsibility. There must be a clear division of roles and responsibility. This will be a tremendous help when dealing with any security issues. Everyone should be subject to the organization's security policy, including employees, management, consultants, and vendors. The following list describes some general areas of responsibility. Specific roles have unique requirements. Some key players and their responsibilities are as follows:

- **Data Owner**—Because senior management is ultimately responsible for data and can be held liable if it is compromised, the data owner is usually a member of senior management, or head of that department. The data owner is responsible for setting the data's security classification. The data owner can delegate some day-to-day responsibility.
- **Data Custodian**—Usually a member of the IT department. The data custodian does not decide what controls are needed, but does implement controls on behalf of the data owner. Other responsibilities include the day-to-day management of data, controlling access, adding and removing privileges for individual users, and ensuring that the proper controls have been implemented.
- **IS Security Steering Committee**—These are individuals from various levels of management that represent the various departments of the organization. They meet to discuss and make recommendations on security issues.
- **Senior Management**—These individuals are ultimately responsible for the security practices of the organization. Senior management might delegate day-to-day responsibility to another party or someone else, but cannot delegate overall responsibility for the security of the organization's data.
- **Security Advisory Group**—These individuals are responsible for reviewing security issues with the chief security officer and they are also responsible for reviewing security plans and procedures.
- **Chief Security Officer**—The individual responsible for the day-to-day security of the organization and its critical assets.
- **Users**—This is a role that most of us are familiar with because this is the end user in an organization. Users do have responsibilities; they must comply with the requirements laid out in policies and procedures.
- **Developers**—These individuals develop code and applications for the organization. They are responsible for implementing the proper security controls within the programs they develop.

- **Auditor**—This individual is responsible for examining the organization's security procedures and mechanisms. The auditor's job is to provide an independent objective as to the effectiveness of the organization's security controls. How often this process is performed depends on the industry and its related regulations. As an example, the health care industry in the United States is governed by the Health Insurance Portability and Accountability Act (HIPAA) regulations and requires yearly reviews.

ExamAlert

The CISSP candidate might be tested on the concept that data access does not extend indefinitely. It is not uncommon for an employee to gain more and more access over time while moving to different positions within a company. Such poor management can endanger an organization. When employees are terminated, data access should be withdrawn. If unfriendly termination is known in advance, access should be terminated as soon as possible to reduce the threat of potential damage.

Data Ownership

All data objects within an organization must have an owner. Objects without a data owner will be left unprotected. The process of assigning a data owner and set of controls to information is known as information lifecycle management (ILM). ILM is the science of creating and using policies for effective information management. ILM includes every phase of a data object from its creation to its end. This applies to any and all information assets.

ILM is focused on fixed content or static data. While data may not stay in a fixed format throughout its lifecycle there will be times when it is static. As an example consider this book; after it has been published it will stay in a fixed format until the next version is released.

For the purposes of business records, there are five phases identified as being part of the lifecycle process. These include the following:

- Creation and Receipt
- Distribution
- Use
- Maintenance
- Disposition

Data owners typically have legal rights over the data. The data owner typically is responsible for understanding the intellectual property rights and copyright of their data. Intellectual property is agreed on and enforced worldwide by various organizations, including the United Nations Commission on International Trade Law (UNCITRAL), the European Union (EU), and the World Trade Organization (WTO). International property laws protect trade secrets, trademarks, patents, and copyrights:

- **Trade secret**—A *trade secret* is a confidential design, practice, or method that must be proprietary or business related. For a trade secret to remain valid, the owner must take precautions to ensure the data remains secure. Examples include encryption, document marking, and physical security.
- **Trademark**—A *trademark* is a symbol, word, name, sound, or thing that identifies the origin of a product or service in a particular trade. The ISC^2 logo is an example of a trademarked logo. The term *service mark* is sometimes used to distinguish a trademark that applies to a service rather than to a product.
- **Patent**—A *patent* documents a process or synthesis and grants the owner a legally enforceable right to exclude others from practicing or using the invention's design for a defined period of time.
- **Copyright**—A *copyright* is a legal device that provides the creator of a work of authorship the right to control how the work is used and protects that person's expression on a specific subject. This includes the reproduction rights, distribution rights, music, right to create, and right to public display.

Data Custodians

Data custodians are responsible for the safe custody, transport, and storage of data and the implementation of business rules. This can include the practice of due care and the implementation of good practices to protect intellectual assets such as patents or trade secrets. Some common responsibilities for a data custodian include the following:

- **Data owner identification**—A data owner must be identified and known for each data set and be formally appointed. Too many times data owners do not know that they are data owners and do not understand the role and its responsibilities. In many organizations the data custodian or IT department by default assumes the role of data owner.
- **Data controls**—Access to data is authorized and managed. Adequate controls must be in place to protect the confidentiality, integrity, and

availability of the data. This includes administrative, technical, and physical controls.

- **Change control**—A change control process must be implemented so that change and access can be audited.
- **End-of-life provisions or disposal**—Controls must be in place so that when data is no longer needed or is not accurate it can be destroyed in an approved method.

Data Documentation and Organization

Data that is organized and structured can help ensure that that it is better understood and interpreted by users. Data documentation should detail how data was created, what the context is for the data, the format of the data and its contents, and any changes that have occurred to the data. It's important to document the following:

- Data context
- Methodology of data collection
- Data structure and organization
- Validity of data and quality assurance controls
- Data manipulations through data analysis from raw data
- Data confidentiality, access, and integrity controls

Data Warehousing

A *data warehouse* is a database that contains data from many other databases. This allows for trend analysis and marketing decisions through data analytics (discussed below). Data warehousing is used to enable a strategic view. Because of the amount of data stored in one location, data warehouses are tempting targets for attackers who can comb through and discover sensitive information.

Data Mining

Data mining is the process of analyzing data to find and understand patterns and relationships about the data (see Figure 2.2). There are many things that must be in place for data mining to occur. These include multiple data sources, access, and warehousing. Data becomes information, information becomes knowledge, and knowledge becomes intelligence through a process called data analytics, which is simply examination of the data. *Metadata* is best described

as being "data about data". As an example, the number 212 has no meaning by itself. But, when qualifications are added, such as to state the field is an area code, it is then understood the information represents an area code on Manhattan Island. Organizations treasure data and the relationships that can be deduced between individual elements. The relationships discovered can help companies understand their competitors and the usage patterns of their customers, and can result in targeted marketing. As an example, it might not be obvious why the diapers are at the back of the store by the beer case until you learn from data mining that after 10 p.m., more men than women buy diapers, and that they tend to buy beer at the same time.

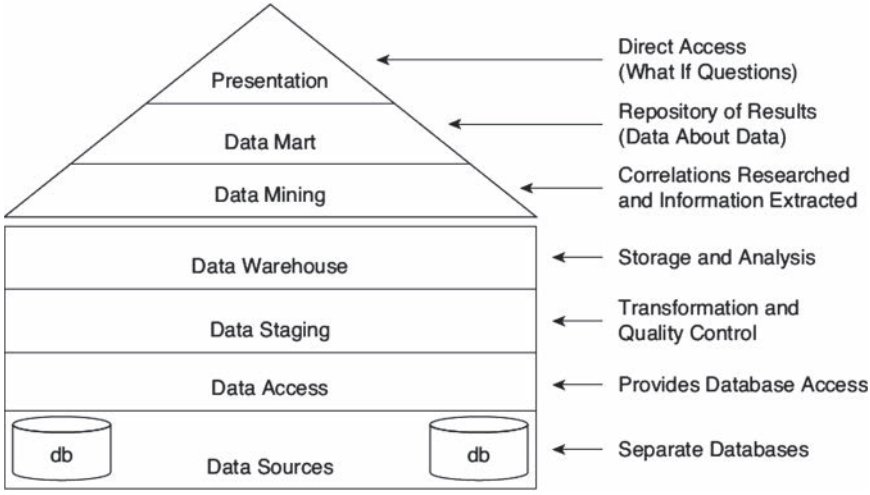

FIGURE 2.2 **Data mining.**

Knowledge Management

Knowledge management seeks to make intelligent use of all the data in an organization by applying wisdom to it. This is called turning data into intelligence through analytics. This skill attempts to tie together databases, document management, business processes, and information systems. The result is a huge store of data that can be mined to extract knowledge using artificial intelligence techniques. These are the three main approaches to knowledge extraction:

- **Classification approach**—Used to discover patterns; can be used to reduce large databases to only a few individual records or data marts. Think of data marts as small slices of data from the data warehouse.

- **Probabilistic approach**—Used to permit statistical analysis, often in planning and control systems or in applications that involve uncertainty.
- **Statistical approach**—A number-crunching approach; rules are constructed that identify generalized patterns in the data.

Data Standards

Data standards provide consistent meaning to data shared among different information systems, programs, and departments throughout the product's life cycle. Data standards are part of any good enterprise architecture. The use of data standards makes data much easier to use. As an example, say you get a new 850-lumen flashlight that uses two AA batteries. You don't need to worry about what brand of battery you buy as all AA batteries are manufactured to the same size and voltage.

Tip

If you would like to see an example of a data standard check out Texas Education Agency. It requires all Texas school districts to submit data to the PEIMS data standard. Learn more at: tea.texas.gov/Reports_and_Data/Data_Submission/PEIMS/PEIMS_Data_Standards/PEIMS_Data_Standards/

Data Lifecycle Control

Data lifecycle control is a policy-based approach to managing the flow of an information system's data throughout its life cycle from the point of creation to the point at which it is out of date and is destroyed or archived.

Data Audit

After all the previous tasks discussed in this chapter have been performed, the organization's security-management practices will need to be evaluated periodically. This is accomplished by means of an *audit process*. The audit process can be used to verify that each individual's responsibility is clearly defined. Employees should know their accountability and their assigned duties. Most audits follow a code or set of documentation. As an example, financial audits can be performed using Committee of Sponsoring Organizations of the Treadway Commission (COSO). IT audits typically follow the Information Systems Audit and Control Association (ISACA) Control Objectives for

Information and related Technology (COBIT) framework. COBIT is designed around four domains:

- Plan and organize
- Acquire and implement
- Deliver and support
- Monitor and evaluate

Although the CISSP exam will not expect you to understand the inner workings of COBIT, you should understand that it is a framework to help provide governance and assurance. COBIT was designed for performance management and IT management. It is considered a system of best practices. COBIT was created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992.

Although auditors can use COBIT, it is also useful for IT users and managers designing controls and optimizing processes. It is designed around 34 key controls that address:

- Performance concerns
- IT control profiling
- Awareness
- Benchmarking

Audits are the only way to verify that the controls put in place are working, that the policies that were written are being followed, and that the training provided to the employees actually works. To learn more about COBIT, check out www.isaca.org/cobit/. Another set of documents that can be used to benchmark the infrastructure is the family of ISO 27000 standards.

Data Storage and Archiving

Organizations have a never-ending need for increased storage. My first 10-megabyte thumb drive is rather puny by today's standards. Data storage can include:

- Network attached storage (NAS)
- Storage area network (SAN)
- Cloud

Organizations should fully define their security requirements for data storage before a technology is deployed. For example, NAS devices are small, easy to use, and can be implemented quickly, but physical security is a real concern, as is implementing strong controls over the data. A SAN can be implemented with much greater security than a NAS. Cloud-based storage offers yet another option but also presents concerns such as:

- Is it a private or public cloud?
- Does it use physical or virtual servers?
- How are the servers provisioned and decommissioned?
- Is the data encrypted and if so what kind of encryption is used?
- Where is the data actually stored?
- How is the data transferred (data flow)?
- Where are the encryption keys kept?
- Are there co-tenants?

Keep in mind that storage integration also includes securing virtual environments, services, applications, appliances, and equipment that provide storage.

SAN

The Storage Network Industry Association (SNIA) defines a SAN as "a data storage system consisting of various storage elements, storage devices, computer systems, and/or appliances, plus all the control software, all communicating in efficient harmony over a network." A SAN appears to the client OS as a local disk or volume that is available to be formatted and used locally as needed.

- **Virtual SAN**—A virtual SAN (VSAN) is a SAN that offers isolation among devices that are physically connected to the same SAN fabric. A VSAN is sometimes called fabric virtualization. VSANs were developed to support independent virtual fabrics on a single switch. VSANs improve consolidation and simplify management by allowing for more efficient SAN utilization. A VSAN will allow a resource on any individual VSAN to be shared by other users on a different VSAN without merging the SAN fabrics.
- **Internet Small Computer System Interface (iSCSI)**—iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. Many see it as a replacement for

fiber channel, because it does not require any special infrastructure and can run over existing IP LAN, MAN, or WAN networks.

- **Fiber Channel over Ethernet (FCoE)**—FCoE is another transport protocol that is similar to iSCSI. FCoE can operate at speeds of 10 GB per second and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. iSCSI is, by contrast, routable because it operates higher up the stack, on top of the TCP and UDP protocols.
- **Host Bus Adapter (HBA) Allocation**—The host bus adapter is used to connect a host system to an enterprise storage device. HBAs can be allocated by either soft zoning or by persistent binding. Soft zoning is more permissive, whereas persistent binding decreases address space and increases network complexity.
- **LUN Masking**—LUN masking is implemented primarily at the HBA level. It is a number system that makes LUN numbers available to some but not to others. LUN masking implemented at this level is vulnerable to any attack that compromises the local adapter.
- **Redundancy (Location)**—Location redundancy is the idea that content should be accessible from more than one location. An extra measure of redundancy can be provided by means of a replication service so that data is available even if the main storage backup system fails.
- **Secure Storage Management and Replication**—Secure storage management and replication systems are designed to allow an organization to manage and handle all its data in a secure manner with a focus on the confidentiality, integrity, and availability of the data. The replication service allows the data to be duplicated in real time so that additional fault tolerance is achieved.
- **Multipath Solutions**—Enterprise storage multipath solutions reduce the risk of data loss or lack of availability by setting up multiple routes between a server and its drives. The multipath software maintains a listing of all requests, passes them through the best possible path, and reroutes communication if a path fails.
- **SAN Snapshots**—SAN snapshot software is typically sold with SAN solutions and offers a way to bypass typical backup operations. The snapshot software has the ability to temporarily stop writing to physical disk and then make a point-in-time backup copy. Snapshot software is typically fast and makes a copy quickly, regardless of the drive size.

- **Data De-Duplication (DDP)**—Data de-duplication is the process of removing redundant data to improve enterprise storage utilization. Redundant data is not copied. It is replaced with a pointer to the one unique copy of the data. Only one instance of redundant data is retained on the enterprise storage media, such as disk or tape.

Data Security, Protection, Sharing, and Dissemination

Data security is the protection of data from unauthorized activity by authorized users and from access by unauthorized users. Although laws differ depending on which country an organization is operating in, organizations must make the protection of personal information in particular a priority. To understand the level of importance, consider that according to the Privacy Rights Clearinghouse (www.privacyrights.org), the total number of records containing sensitive personal information accumulated from security breaches in the United States between January 2005 and December 2015 is 895,531,860.

From a global standpoint the international standard ISO/IEC 17799 covers data security. ISO 17799 makes clear the fact that all data should have a data owner and data custodian so that it is clear whose responsibility it is to secure and protect access to that data.

An example of a proprietary international information security standard is the Payment Card Industry Data Security Standard. PCI-DSS sets standards for any entity that handles cardholder information for credit cards, prepaid cards, and POS cards. PCI DSS version is comprised of six control objectives that contain one or more requirements:

1. Build and Maintain a Secure Network

   Requirement 1: Install and maintain a firewall configuration to protect cardholder data

   Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2. Protect Cardholder Data

   Requirement 3: Protect stored cardholder data

   Requirement 4: Encrypt transmission of cardholder data across open, public networks

3. Maintain a Vulnerability Management Program

   Requirement 5: Use and regularly update anti-virus software

   Requirement 6: Develop and maintain secure systems and applications

4. Implement Strong Access Control Measures

   Requirement 7: Restrict access to cardholder data by business need-to-know

   Requirement 8: Assign a unique ID to each person with computer access

   Requirement 9: Restrict physical access to cardholder data

5. Regularly Monitor and Test Networks

   Requirement 10: Track and monitor all access to network resources and cardholder data

   Requirement 11: Regularly test security systems and processes

6. Maintain an Information Security Policy

   Requirement 12: Maintain a policy that addresses information security

Privacy Impact Assessment

Another approach for organizations seeking to improve their protection of personal information is to develop an organization-wide policy based on a *privacy impact analysis* (PIA). A PIA should determine the risks and effects of collecting, maintaining, and distributing personal information in electronic-based systems. The PIA should be used to evaluate privacy risks and ensure that appropriate privacy controls exist. Existing data controls should be examined to verify that accountability is present and that compliance is built-in every time new projects or processes are planned to come online. The PIA must include a review of the following items as they adversely affect the CIA of privacy records:

- **Technology**—Any time new systems are added or modifications are made, reviews are needed.
- **Processes**—Business processes change, and even though a company might have a good change policy, the change management system might be overlooking personal information privacy.
- **People**—Companies change employees and others with whom they do business. Any time business partners, vendors, or service providers change, the impact of the change on privacy needs to be reexamined.

Privacy controls tend to be overlooked for the same reason many security controls are. Management might have a preconceived idea that security controls will reduce the efficiency or speed of business processes. To overcome these types of barriers, senior management must make a strong commitment to protection of personal information and demonstrate its support. Risk-assessment activities aid in the process by informing stakeholders of the actual costs for the loss of personal information of clients and customers. These costs can include fines, lawsuits, lost customers, reputation, and the company going out of business.

Information Handling Requirements

Organizations handle large amounts of information and should have policies and procedures in place that detail how information is to be stored. Think of policies as high level documents, whereas procedures offer step-by-step instructions. Many organizations are within industries that fall under regulatory standards that detail how and how long information must be retained.

One key concern with storage is to ensure that media is appropriately labeled. Media should be labeled so that the data librarian or individual in charge of media management can identify the media owner, when the content was created, the classification level, and when the content is to be destroyed. Figure 2.3 shows an example of appropriate media labeling.

FIGURE 2.3 **Data labeling.**

Data Retention and Destruction

All data has a lifetime. Eventually it should either be purged, released, or unclassified. As an example, consider the JFK Records Act. The JFK Records Act was put in place to eventually declassify all records dealing with the assassination of President John F. Kennedy. The JFK Records Act states that all assassination records must finally be made public by 2017. This is an example of declassification, but sometimes data in an organization will never be released and will need to be destroyed.

If the media is held on hard drives, magnetic media, or thumb drives, it must be sanitized. *Sanitization* is the process of clearing all identified content, such that no data remnants can be recovered. Some of the methods used for sanitization are as follows:

- **Drive wiping**—This is the act of overwriting all information on the drive. As an example, DoD.5200.28-STD (7) specifies overwriting the drive with a special digital pattern through seven passes. Drive wiping allows the drive to be reused.
- **Zeroization**—This process is usually associated with cryptographic processes. The term was originally used with mechanical cryptographic devices. These devices would be reset to 0 to prevent anyone from recovering the key. In the electronic realm, *zeroization* involves overwriting the data with zeros. Zeroization is defined as a standard in ANSI X9.17.
- **Degaussing**—This process is used to permanently destroy the contents of a hard drive or magnetic media. Degaussing works by means of a powerful magnet whose field strength penetrates the media and reverses the polarity of the magnetic particles on the tape or hard disk. After media has been degaussed, it cannot be reused. The only method more secure than degaussing is physical destruction.

Data Disposal is a Big Problem

While hard drive size and performance has continued to grow at a rapid pace most hard drive and thumb drives are still shipped without encryption enabled. What this means is that you can take a hard drive from a computer you bought at an auction that will not boot up, plug the drive into another computer, and possibly have access to the data on the drive. While many of us have used a shredder, few have probably ever sanitized a hard drive. Whether your organization is planning to sell old hard drives, give them to charity, or just throw them away, you need to make sure the data on the drive is impossible to recover.

If you are thinking that most organizations already do this, consider the following. Two researchers from MIT bought 158 used hard drives from eBay. Out of the 158 hard drives, 129 had data that the researchers were able to copy. Some of the data on these drives included personal information, company HR records, medical information, a pharmacies database, and another database with 3,700 credit card numbers.

Physical media should be protected with a level of control equal to electronic media. These issues are covered in much greater detail in Chapter 3, "Physical Asset Security."

With the discussion of controls concluded, the next section focuses on auditing and monitoring. It is time to review some of the ways organizations can maintain accountability.

Note

Unless you're a 1960s car enthusiast like I am, it might have been a while since you have seen a working 8-track player. The point is that technology changes and the requirement to be able to read and access old media is something to consider. Be it 8-tracks, laser discs, Zip drives, or floppy disks, stored media must be readable to be useful.

Data Remanence and Decommissioning

Object reuse is important because of the remaining information that may reside on a hard disk or any other type of media. Even when data has been sanitized there may be some remaining information. This is known as data remanence. Data remanence is the residual data that remains after data has been erased. Most objects that may be reused will have some remaining amount of information left on media after it has been erased. If the media is not going to be destroyed outright, best practice is to overwrite it with a minimum of seven passes of random ones and zeros.

When information is deemed too sensitive assets such as hard drive, media, and other storage devices may not be reused and the decision may be made for asset disposal. Asset disposal must be handled in an approved manner and part of the system development life cycle. As an example, media that has been used to store sensitive or secret information should be physically destroyed. Before systems or data are decommissioned or disposed of, you must understand any existing legal requirements pertaining to records retention. When archiving information, you must consider the method for retrieving the information.

Classifying Information and Supporting Assets

Organizational information that is proprietary or confidential in nature must be protected. Data classification is a useful way to rank an organization's informational assets. A well-planned data classification system makes it easy to store and access data. It also makes it easier for users of data to understand its importance. As an example, if an organization has a clean desk policy and mandates that company documents, memos, and electronic media not be left on desks, it can change people's attitudes about the value of that information. However, whatever data classification system is used, it should be simple enough that all employees can understand it and execute it properly. Two common data classification plans are discussed next.

Data Classification

The two most common data-classification schemes are military and public. Organizations store and process so much electronic information about their customers and employees that it's critical for them to take appropriate precautions to protect this information. The responsibility for the classification of data lies with the data owner. Both military and private data classification systems accomplish this task by placing information into categories and applying labels to data and clearances to people that access the data.

The first step of this process is to assess the value of the information. When the value is known, it becomes much easier to decide the amount of resources that should be used to protect the data. It would make no sense to spend more on protecting something with a lesser value. By using this system, not all data is treated equally; data that requires more protection gets it, and funds are not wasted protecting data that does not need it.

Each level of classification established should have specific requirements and procedures. The military and commercial data-classification models have predefined labels and levels. When an organization decides which model to use, it can evaluate data placement by using criteria such as the following:

- Data value
- Data age
- Laws pertaining to data

- Regulations pertaining to disclosure
- Replacement cost

Regardless of which model is used, the following questions will help determine the proper placement of the information:

- Who owns the asset or data?
- Who controls access rights and privileges?
- Who approves access rights and privileges?
- What level of access is granted to the asset or data?
- Who currently has access to the asset or data?

Classification of data requires several steps:

1. Identify the data custodian.
2. Determine the criteria used for data classification.
3. Task the owner with classifying and labeling the information.
4. Identify any exceptions to the data classification policy.
5. Determine security controls to be applied to protect each category of information.
6. Specify sunset policy or end of life policy and detail in a step-by-step manner how data will be reclassified or declassified. Reviews specifying rentention and end of life should occur at specific periods of time.
7. Develop awareness program.

Military Data Classification

The military data-classification system is mandatory within the U.S. Department of Defense. This system has five levels of classification:

- **Top Secret**—Grave damage if exposed.
- **Secret**—Serious damage if exposed.
- **Confidential**—Disclosure could cause damage.
- **Sensitive but Unclassified or Restricted**—Disclosure should be avoided.
- **Unclassified or Official**—If released, no damage should result.

Each classification represents a level of sensitivity. *Sensitivity* is the desired degree of secrecy that the information should maintain. If you hold a confidential clearance, it means that you could access unclassified, sensitive, or confidential information for which you have a need to know. Your need to know would not extend to the secret or top secret levels. The concept of need-to-know is similar to the principle of least privilege in that employees should have access only to information that they need to know to complete their assigned duties.

Public/Private Data Classification

The public or commercial data classification is also built on a four-level model:

- **Confidential**—This is the highest level of sensitivity and disclosure could cause extreme damage to the organization.
- **Private**—This information is for organization use only and its disclosure would damage the organization.
- **Sensitive**—This information requires a greater level of protection to prevent loss of confidentiality.
- **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.

Table 2.1 provides details about the military and public/private data-classification models.

TABLE 2.1 **Commercial and Military Data Classifications**

Commercial Business Classifications	Military Classifications
Confidential	Top secret
Private	Secret
Sensitive	Confidential
Public	Sensitive (BU)
	Unclassified

Caution

Information has a useful life. Data classification systems need to build in mechanisms to monitor whether information has become obsolete. Obsolete information should be declassified or destroyed.

Asset Management and Governance

The job of asset management and governance is to align the goals of IT to the business functions of the organization, to track assets throughout their life-cycle, and to protect the assets of the organization. Asset management can be defined as any system that inventories, monitors, and maintains items of value. Assets can be both tangible and intangible. Assets can include the following:

- Hardware
- Software
- Employees
- Services
- Reputation
- Documentation

You can think of asset management as a structured approach of deploying, operating, maintaining, upgrading, and disposing of assets cost-effectively. Asset management is required for proper risk assessment. Before you can start to place a value on an asset you must know what it is and what it is worth. Its value can be assessed either quantitatively or qualitative. A quantitative approach requires:

1. Estimation of potential losses and determination of single loss expectancy (SLE)
2. Completion of a threat frequency analysis and calculation of the annual rate of occurrence (ARO)
3. Determination of the annual loss expectancy (ALE)

A qualitative approach does not place a dollar value on the asset and ranks it as high, medium, or low concern. The downside of performing qualitative evaluations is that you are not working with dollar values, so it is sometimes harder to communicate the results of the assessment to management.

One key asset is software. CISSP candidates should understand common issues related to software licensing. Because software vendors usually license their software rather than sell it, and license it for a number of users on a number of systems, software licenses must be accounted for by the purchasing organization. If users or systems exceed the licensed number, the organization can be held legally liable.

As we move into an age where software is being delivered over the Internet and not with media (CD), software asset management is an important concern.

Software Licensing

Intellectual property rights issues have always been hard to enforce. Just consider the uproar that Napster caused years ago as the courts tried to work out issues of intellectual property and the rights of individuals to share music and files. The software industry has long dealt with this same issue. From the early days of computing, some individuals have been swapping, sharing, and illegally copying computer software. The unauthorized copying and sharing of software is considered software piracy, which is illegal. Many don't think that the copy of that computer game you gave a friend is hurting anyone. But software piracy is big business, and accumulated loss to the property's owners is staggering. According to a 2008 report on intellectual property to the United States Congress, in just one raid in June 2007, the FBI recovered more than two billion dollars worth of illegal Microsoft and Symantec software. Internationally, losses from illegal software are estimated to be in excess of $200 billion.

Microsoft and other companies are actively fighting to protect their property rights. Some organizations have formed the Software Protection Association, which is one of the primary bodies that work to enforce licensing agreements. The Business Software Alliance (BSA) and the Federation Against Software Theft are international groups targeting software piracy. These associations target organizations of all sizes from small, two-person companies to large multinationals.

Software companies are making clear in their licenses what a user can and cannot do with their software. As an example, Microsoft Windows XP allowed multiple transfers of licenses whereas Windows 8 and 10 have different transfer rules. As an example, Windows 8 allows only one transfer. The user license states, "The first user of the software may reassign the license to another device one time." Some vendors even place limits on virtualization. License agreements can actually be distributed in several different ways, including the following:

- **Click-wrap license agreements**—Found in many software products, these agreements require you to click through and agree to terms to install the software product. These are often called *contracts of adhesion*; they are "take it or leave it" propositions.
- **Master license agreements**—Used by large companies that develop specific software solutions that specify how the customer can use the product.

- **Shrink-wrap license agreements**—Created when software started to be sold commercially and named for the fact that breaking the shrink wrap signifies your acceptance of the license.

Even with licensing and increased policing activities by organizations such as the BSA, improved technologies make it increasingly easy to pirate software, music, books, and other types of intellectual property. These factors and the need to comply with two World Trade Organization (WTO) treaties led to the passage of the 1998 Digital Millennium Copyright Act (DMCA). Here are some salient highlights:

- The DMCA makes it a crime to bypass or circumvent antipiracy measures built into commercial software products.
- The DMCA outlaws the manufacture, sale, or distribution of any equipment or device that can be used for code-cracking or illegally copying software.
- The DMCA provides exemptions from anti-circumvention provisions for libraries and educational institutions under certain circumstances; however, for those not covered by such exceptions, the act provides penalties up to $1,000,000 and 10 years in prison.
- The DMCA provides Internet service providers exceptions from copyright infringement liability enabling transmission of information across the Internet.

Equipment Lifecycle

The equipment lifecycle begins at the time equipment is requested to the end of its useful life or when it is discarded. The equipment lifecycle typically consist of four phases:

- Defining requirements
- Acquisition and implementation
- Operation and maintenance
- Disposal and decommission

While some may think that much of the work is done once equipment has been acquired, that is far from the truth. There will need to be some established support functions. Routine maintenance is one important item.

Without routine maintenance equipment will fail, and those costs can be calculated. Items to consider include:

- Lost productivity
- Delayed or canceled orders
- Cost of repair
- Cost of rental equipment
- Cost of emergency services
- Cost to replace equipment or reload data
- Cost to pay personnel to maintain the equipment

Technical support is another consideration. The longer a piece of equipment has been in use the more issues it may have. As an example, if you did a search for exploits for Windows 7 or Windows 10 which do you think would return more results? Most likely Windows 7. This all points to the need for more support the longer the resource has been in use.

Determine Data Security Controls

Any discussion on logical asset security must at some point discuss encryption. While there is certainly more to protecting data than just encrypting it, encryption is one of the primary controls used to protect data. Just consider all the cases of lost hard drives, laptops, and thumb drives that have made the news because they contained data that was not encrypted. In many cases encryption is not just a good idea; it is also mandated by law. CISSP candidates must ensure that corporate policies addressing where and how encryption will be used are well defined and being followed by all employees.

Let's examine the two areas at which encryption can be used to protect data at a high level. These topics will be expanded on in Chapter 6, "The Application and Use of Cryptography."

Data at Rest

Data at rest is information stored on some form of media that is not traversing a network or residing in temporary memory. Failure to properly protect data at rest can lead to attacks such as the following:

- Pod slurping, a technique for illicitly downloading or copying data from a computer. Typically used for data exfiltration.

- Various forms of USB (Universal Serial Bus) malware, including but not limited to USB Switchblade and Hacksaw.
- Other forms of malicious software, including but not limited to viruses, worms, Trojans, and various types of key loggers.

Data at rest can be protected via different technical and physical hardware or software controls that should be defined in your security policy. Some hardware offers the ability to build in encryption. A relatively new hardware security device for computers is called the *trusted platform module* (TPM) chip. The TPM is a "slow" cryptographic hardware processor which can be used to provide a greater level of security than software encryption. A TPM chip installed on the motherboard of a client computer can also be used for system state authentication. The TPM can also be used to store the encryption keys.

The TPM measures the system and stores the measurements as it traverses through the boot sequence. When queried, the TPM will return these values signed by a local private key. These values can be used to discover the status of a platform. The recognition of the state and validation of these values is referred to as *attestation*. Phrased differently, attestation allows one to confirm, authenticate, or prove a system to be in a specific state. Data can also be encrypted using these values. This process is referred to as *sealing a configuration*. In short, the TPM is also a tamper-resistant cryptographic module that can provide a means to report the system configuration to a policy enforcer or "health monitor."

The TPM also provides the ability to encrypt information to a specific platform configuration by calculating hashed values based on items such as the system's firmware, configuration details, and core components of the operating system as it boots. These values, along with a secret key stored in the TPM, can be used to encrypt information and only allow it to become usable in a specific machine configuration. This process is called *sealing*.

The TPM is now addressed by ISO 11889-1:2009. It can also be used with other forms of data and system protection to provide a layered approach, referred to as defense in depth. For example, the TPM can help protect the actual system, while another set of encryption keys can be stored on a user's common access card or smart card to decrypt and access the data set.

Another potential option that builds on this technology is self-encrypting hard drives (SEDs). These pieces of hardware offer many advantages over non-encrypted drives:

- Compliance—SEDs have the ability to offer built-in encryption. This can help with compliance laws that many organizations must adhere to.

- Strong security—SEDs make use of strong encryption. The contents of an SED are always encrypted and the encryption keys are themselves encrypted and protected in hardware.
- Ease of use—Users only have to authenticate to the drive when the device boots up or when they change passwords/credentials. The encryption is not visible to the user.
- Performance—As SEDs are not visible to the user and are integrated into hardware, the system operates at full performance with no impact on user productivity.

Software encryption is another protection mechanism for data at rest. There are many options available, such as EFS, BitLocker, and PGP. Software encryption can be used on specific files, databases, or even entire RAID arrays that store sensitive data. What is most important about any potential software option is that not only must the encrypted data remain secure and remain inaccessible when access controls, such as usernames and passwords, are incorrect; the encryption keys themselves must be protected, and should therefore be updated on a regular basis.

Caution

Encryption keys should be stored separately from the data.

Data in Transit

Any time data is being processed or moved from one location to the next, it requires proper controls. The basic problem is that many protocols and applications send information via clear text. Services such as email, web, and FTP were not designed with security in mind and send information with few security controls and no encryption. Examples of insecure protocols include:

- FTP—Clear-text username and password
- Telnet—Clear-text username and password
- HTTP—Clear text
- SMTP—All data is passed in the clear

For data in transit that is not being protected by some form of encryption, there are many dangers, which include the following:

- Eavesdropping
- Sniffing

- Hijacking
- Data alteration

Today, many people connect to corporate networks from many different locations. Employees may connect via free Wi-Fi from coffee shops, restaurants, airports, or even hotels.

One way to protect this type of data in transit is by means of a Virtual Private Network (VPN). VPNs are used to connect devices through the public Internet. Three protocols are used to provide a tunneling mechanism in support of VPNs: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IP Security (IPSec). When an appropriate protocol is defined, the VPN traffic will be encrypted. Microsoft supplies Microsoft Point-to-Point Encryption (MPPE), with PPTP, native to the Microsoft operating systems. L2TP offers no encryption, and as such is usually used with IPSec in ESP mode to protect data in transit. IPSec can provide both tunneling and encryption.

Two types of tunnels can be implemented:

- **LAN-to-LAN tunnels**—Users can tunnel transparently to each other on separate LANS.
- **Host-to-LAN tunnels**—Mobile users can connect to the corporate LAN.

Having an encrypted tunnel is just one part of protecting data in transit. Another important concept is that of authentication. Almost all VPNs use digital certificates as the primary means of authentication. X.509 v3 is the de facto standard. X.509 specifies certificate requirements and their contents. Much like that of a state driver's license office, the Certificate Authority (CA) guarantees the authenticity of the certificate and its contents. These certificates act as an approval mechanism.

Just as with other services, organizations need to develop policies to define who will have access to the VPN and what encryption mechanisms will be used. It's important that VPN policies be designed to map to the organization's security policy. As senior management is ultimately responsible, they must approve and support this policy.

Standard email is also very insecure and can be exposed while in transit. Standard email protocols such as SMTP, POP3, and IMAP all send data via clear text. To protect email in transit you must use encryption. Email protection mechanisms include PGP, Secure Multipurpose Internet Mail Extensions (S/MIME), and Privacy Enhanced Mail (PEM). Regardless of what is being protected periodic auditing of sensitive data should be part of policy and should occur on a regular schedule.

Data in transit will also require a discussion of how the encryption will be applied. Encryption can be performed at different locations with different amounts of protection applied.

- **Link encryption**—The data is encrypted through the entire communication path. Because all header information is encrypted each node must decrypt and encrypt the routing information. Source and destination address cannot be seen to someone sniffing traffic.
- **End to end encryption**—Generally performed by the end user and as such can pass through each node without further processing. However, source and destination addresses are passed in clear text, so they can be seen to someone sniffing traffic.

Endpoint Security

No review of logical asset security would be complete without a discussion of endpoint security. Endpoint security consists of the controls placed on client or end user systems, such as control of USB and CD/DVD, antivirus, anti-malware, anti-spyware, and so on. The controls placed on a client system are very important.

- Removable media—A common vector for malware propagation is via USB thumb drive. Malware such as Stuxnet, Conficker, and Flame all had the capability to spread by thumb drives. Removable drives should be restricted and turned off when possible.
- Disk encryption—Disk encryption software such as EFS and BitLocker can be used to encrypt the contents of desktop and laptop hard drives. Also, corporate smartphones and tablets should have encryption enabled.
- Application whitelisting—This approach only allows known good applications and software to be installed, updated, and used. Whitelisting techniques can include code signing, digital certificates, known good cryptographic hashes, or trusted full paths and names. Blacklisting, alternatively, blocks known bad software from being downloaded and installed.
- Host-based firewalls—Defense in depth dictates that the company should consider not just enterprise firewalls but also host-based firewalls.
- Configuration lockdown—Not just anyone should have the ability to make changes to equipment or hardware. Configurations controls can be used to prevent unauthorized changes.
- Antivirus—This is the most commonly deployed endpoint security product. While it is a needed component, antivirus has become much less effective over the last several years.

One basic starting point is to implement the principle of least privilege. This concept can also be applied to each logical asset: each computer, system component or process should have the least authority necessary to perform its duties.

Baselines

A baseline can be described as a standard of security. Baselines are usually mapped to industry standards. As an example, an organization might specify that all computer systems be certified by Common Criteria to an Evaluation Assurance Level (EAL) 3. Another example of baselining can be seen in NIST 800-53. NIST 800-53 describes a tailored baseline as a starting point for determining the needed level of security as seen in Figure 2.4.

- IT structure analysis (survey)—Includes analysis of technical, operation, and physical aspects of the organization, division, or group.
- Assessment of protection needs—Determination of the needed level of protection. This activity can be quantitative or qualitative.
- Selection of actions—Determination of what specific controls need to be implemented.
- Running comparison of nominal and actual—Periodic review of activities and actions to measure the change between what was previously occurring and what is currently occurring.

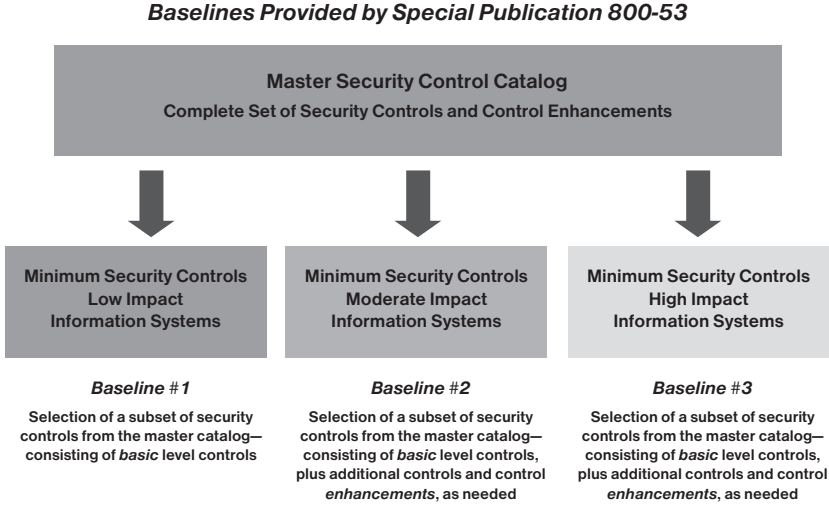

FIGURE 2.4 **NIST 800-53 Scoping and Baselining Controls.**

NIST 800-53 specifies scoping or tailoring activities and categorizes information based on impact.

- Low impact
- Moderate impact
- High impact

Scoping or tailoring is the act of adding or removing controls as needed to get the right level of protection. Obviously, adding controls will increase cost and generally increase system security, whereas removing controls reduces costs but can expose the system to unnecessary threats. Therefore due care must be used to determine the proper level of controls. Scoping and tailoring activities should be well documented with appropriate justification. In some cases, information and information systems must be protected regardless of the cost, because of laws that may govern certain industries.

Laws, Standards, Mandates and Resources

The following laws, standards, and mandates have an impact on information security and can affect the risk profile of an organization. Regardless of the laws and mandates, organizations should be proactive when it comes to corporate governance. Several laws and mandates are described here:

- Health Insurance Portability and Accountability Act (HIPAA)—HIPAA was signed into law in 1996. It has two areas. Title I of the HIPAA of 1996 protects health insurance coverage for workers and their families when they change or lose their jobs. Title II requires the U.S. Department of Health and Human Services (DHHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers.

Under HIPAA, the U.S. DHHS was required to publish a set of rules regarding privacy. The Privacy Rule dictates controls that organizations must put in place to protect personal information. The privacy rule defines three major purposes:

- "To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information."

- "To improve the quality of health care in the United States by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care."
- "To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals."

Gramm-Leach-Bliley Act (GLBA)—GLBA was signed into law in 1999 and resulted in the most sweeping overhaul of financial services regulation in the United States.

Title V of GLBA addresses financial institution privacy with two subtitles. Subtitle A requires financial institutions to make certain disclosures about their privacy policies and to give individuals an opt-out capability. Subtitle B criminalizes the practice known as pretexting, which can be described as the practice of obtaining personal information under false pretenses.

Under GLBA, financial institutions are required to protect the confidentiality of individual privacy information. As specified in GLBA, financial institutions are required to develop, implement, and maintain a comprehensive information security program with appropriate administrative, technical, and physical safeguards. Administrative controls include items such as background checks and separation of duties. Technical controls can be hardware or software, such as encryption or an IDS. Physical controls include gates, guards, and fences. The controls specified in the information security program must include:

- The assignment of a designated program manager for the organization's information security program
- A periodic risk and vulnerability assessment and audit
- A program of regular testing and monitoring
- The development of policies and procedures for control of sensitive information and PII

Federal Information Security Management Act (FISMA)—FISMA was signed into law in 2002. One of the big changes that FISMA brought about was a set of clear guidelines for information security designed for the protection of

federal government IT infrastructure and data assets. FISMA requirements specify the following responsibilities:

- Develop and maintain an information assurance (IA) program with an entire IT security architecture and framework.
- Ensure that information security training is conducted to keep IAT and IAM personnel properly trained and certified in accordance with DoD. 8570.
- Implement accountability for personnel with significant responsibilities for information security.

FISMA also requires periodic risk assessments, risk assessment policies and procedures, periodic (at least annual) testing and evaluation, and proper training and awareness to senior management so that proper security awareness programs can be deployed.

Sarbanes-Oxley Act (SOX)—SOX was signed into law in 2002. This act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. Sections 302 and 404 are the two sections that address IT infrastructures and information security. Section 302 requires the CEO and CFO to personally certify that the organization has the proper internal controls. It also mandates that the CEO and CFO report on effectiveness of internal controls around financial reporting.

Section 404 sets requirements on management's structure, control objectives, and control procedures. Staying compliant with Section 404 requires companies to establish an infrastructure that is designed to archive records and data and protect them from destruction, loss, unauthorized alteration, or other misuse. It requires that a set of comprehensive controls be put in place and holds CEOs and CFOs accountable.

United States Resources

NIST started as the National Bureau of Standards and changed its name in 1989 to the National Institute of Standards and Technology. Some of the NIST documents a CISSP should have knowledge of are:

- NIST 800-37—Guide for applying risk management.
- NIST 800-53—Government publication that provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. Many

organizations in private industry use NIST SP 800-53 as a guide for their own security management.

- NIST 800-60—Guide for Mapping Types of Information and Information.

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.

- FIPS 199—Establishes security categories of information systems used by the federal government.
- FIPS 200—Mandatory security standards for government systems.

International Resources

Our first item is the information technology infrastructure library (ITIL). ITIL provides a framework for identifying, planning, delivering, and supporting IT services for business.

The IT Governance Institute has developed a process that begins with setting objectives for the enterprise's IT, providing the initial direction and then evolving into a continuous loop.

ITIL presents a service lifecycle that includes

- Continual service improvement
- Service strategy
- Service design
- Service transition
- Service operation

Next up are some of the standards from the International Organization for Standardization that a CISSP should be familiar with:

- ISO **27001**—This standard describes requirements on how to establish, implement, operate, monitor, review, and maintain an information security management system (ISMS); it is based on British Standard 7799.
- ISO **27002**—This standard is considered a code of practice that describes ways to develop a security program within the organization.

- ISO **27003**—This standard focuses on implementation.
- ISO **27004**—This standard is a standard for information security measurements.
- ISO **27005**—This standard describes how to implement solutions based on risk management.
- ISO **27799**—This standard describes how to protect personal health information.

ISO 9001 is a quality management standard that has widespread support and attention. ISO 9001 describes how production processes are to be managed and reviewed. It is not a standard of quality; it is about how well a system or process is documented. Companies that wish to obtain 9001 certification will need to perform a gap analysis to determine areas that need improvement. ISO 9001 is actually six documents that specify:

- Control of Documents
- Control of Records
- Control of Non-conforming Product
- Corrective Action
- Preventive Action
- Internal Audits

Tip

Achieving ISO 9001:2000 Certification—ISO 9001 certification requires an organization to perform a gap analysis. This allows the company to identify shortcomings that need to be addressed in order to obtain certification.

Being ISO-certified means that the organization has the capability to provide products that meet specific requirements, and includes a process for continual improvement. It may also have a direct bearing on an audit as it places strong controls on documented procedures. Another ISO standard that the auditor should be aware of is ISO 17799. 17799 provides the best practice guidance on information security management. It is divided into 12 main sections:

- Risk assessment and treatment
- Security policy

- Organization of information security
- Asset management
- Human Resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Tip

CISSP exam candidates should have a basic understanding of ISO standards and their purpose; however, the exam does not cover U.S. laws.

Finally, let's review a couple of European documents:

- 10 Steps to Cyber Security—Detailed cyber-security information and advice across 10 critical technical and procedural areas. Created by CESG, the information security arm of GCHQ, and the National Technical Authority for Information Assurance within the United Kingdom.
- Cybersecurity Strategy of the European Union—This document was developed by the European Union; it describes their approach to preventing and responding to cyber-security attacks.

Exam Prep Questions

1. Which of the following levels best represents the military classification system?
   - ❍ **A.** Confidential, private, sensitive, and public
   - ❍ **B.** Top secret, secret, private, sensitive, and public
   - ❍ **C.** Top secret, confidential, private, sensitive, and unclassified
   - ❍ **D.** Top secret, secret, confidential, sensitive, and unclassified

2. Which of the following standards describes how well a system or process is documented?
   - ❍ **A.** ISO 27001
   - ❍ **B.** ISO 9001
   - ❍ **C.** ISO 27002
   - ❍ **D.** ISO 17799

3. Which of the following endpoint security controls could have been used to potentially prevent malware such as Stuxnet, Conficker, and Flame?
   - ❍ **A.** Implementing disk encryption
   - ❍ **B.** Hardening edge devices
   - ❍ **C.** Blocking removable media
   - ❍ **D.** Enforcing application whitelisting

4. Place the following in their proper order:
   - ❍ **A.** Determine SLE, ARO, and ALE, then asset value.
   - ❍ **B.** Determine asset value, then ARO, SLE, and ALE.
   - ❍ **C.** Determine asset value, then SLE, ALE, and SLE.
   - ❍ **D.** Determine asset value, then SLE, ARO, and ALE.

5. The downside of performing this type of assessment is that you are not working with dollar values, so it is sometimes harder to communicate the results of the assessment to management. Which of the following assessment types does this describe?
   - ❍ **A.** Qualitative
   - ❍ **B.** Quantitative
   - ❍ **C.** Numeric mitigation
   - ❍ **D.** Red team

6. Which of the following categories of control can include the logical mechanisms used to control access and authenticate users?
   - ❍ **A.** Administrative
   - ❍ **B.** Clerical
   - ❍ **C.** Technical
   - ❍ **D.** Physical

7. Which of the following is incorrect when describing an SED?
   - ❍ **A.** Eases compliance
   - ❍ **B.** Slow performance
   - ❍ **C.** Ease of use
   - ❍ **D.** Strong security

8. Which of the following is the top level of protection for commercial business classification?
   - ❍ **A.** Secret
   - ❍ **B.** Confidential
   - ❍ **C.** Top secret
   - ❍ **D.** Private

9. Which of the following is the most specific of security documents?
   - ❍ **A.** Procedures
   - ❍ **B.** Standards
   - ❍ **C.** Policies
   - ❍ **D.** Baselines

10. The last thing you want in an organization is that everyone is accountable but no one is responsible. Therefore, the data owner should be in which of the following groups?
    - ❍ **A.** End users
    - ❍ **B.** Technical managers
    - ❍ **C.** Senior management
    - ❍ **D.** Everyone is responsible; therefore, all groups are owners

11. Which term best describes a symbol, word, name, sound, or thing that uniquely identifies a product or service?

- ❍ **A.** Trade secret
- ❍ **B.** Copyright
- ❍ **C.** Patent
- ❍ **D.** Trademark

12. After opening a new branch in the Midwest your company is analyzing buying patterns to determine the relationship between various items purchased. Which of the following best describes this situation?

- ❍ **A.** Data mining
- ❍ **B.** Knowledge management
- ❍ **C.** Data warehouse
- ❍ **D.** Data standards

13. Which ISO document is used for a standard for information security management?

- ❍ **A.** ISO 27001
- ❍ **B.** ISO 27002
- ❍ **C.** ISO 27004
- ❍ **D.** ISO 27799

14. Which of the following SAN solutions is fast, rides on top of Ethernet, yet is non-routable?

- ❍ **A.** SCSI
- ❍ **B.** iSCSI
- ❍ **C.** HBA
- ❍ **D.** FCoE

15. Who is ultimately responsible for the security of an asset?

- ❍ **A.** Asset owner
- ❍ **B.** Auditor
- ❍ **C.** Custodian
- ❍ **D.** Risk assessment team

Answers to Exam Prep Questions

1. **D.** The military data classification system is widely used within the Department of Defense. This system has five levels of classification: unclassified, sensitive, confidential, secret, and top secret. Each level represents an increasing level of sensitivity.
2. **B.** ISO 9001 describes how production processes are to be managed and reviewed. It is not a standard of quality; it is about how well a system or process is documented. Answers A, C, and D are incorrect: ISO 27001 describes requirements on how to establish, implement, operate, monitor, review, and maintain an information security management system; ISO 27002 is considered a code of practice that describes ways to develop a security program within the organization; ISO 17799 provides best practice guidance on information security management.
3. **C.** Restricting removable media may have helped prevent infection from malware that is known to spread via thumb drive or removable media. Answer A is incorrect because encryption of media would not have helped. Answer B is incorrect because edge devices were not specifically targeted. Answer D is incorrect because enforcing application whitelisting would not have prevented advanced persistent threats from executing on local systems.
4. **D.** The proper order is to determine the asset value, then SLE, ARO, and ALE. Answers A, B, and C are incorrect; they are not in the proper order.
5. **A.** Qualitative assessment is scenario-driven and does not attempt to assign dollar values to components of the risk analysis. Quantitative assessment is based on dollar amounts; both numeric mitigation and red team are distractors.
6. **C.** Technical controls can be hardware or software. They are the logical mechanisms used to control access and authenticate users, identify unusual activity, and restrict unauthorized access. Clerical is a nonexistent category and all other answers are incorrect: administrative controls are procedural and physical controls include locks, guards, gates, and alarms.
7. **B.** Self-encrypting hard drives offer many advantages, such as easing compliance issues with items like PII. They are easy to use and offer strong encryption. Answer B is correct because SEDs do not slow down performance; they are actually integrated into the hardware and operate at full performance with no impact on user productivity.
8. **B.** Confidential is the top level of data classification for commercial business classification. Answers A, C, and D are incorrect because secret and top secret are both part of the military classification, while private is a lower level of commercial business classification.
9. **A.** A procedure is a detailed, in-depth, step-by-step document that lays out exactly what is to be done. It's tied to specific technologies and devices. Standards are tactical documents; policies are high-level documents; and baselines are minimum levels of security that a system, network, or device must adhere to.

10. **C.** Senior management is the ultimate owner because these individuals are responsible for the asset and must answer if data is compromised. Although answer C is the best possible choice, it is important to realize that, in most cases, the data owner will be a member of management but might not be the most senior executive within the organization. For example, the CFO would be the data owner for all financial data, the director of human resources would be the data owner for all HR data, and so on. All other answers are incorrect because end users, technical managers, and other employees are not typically the data owners.
11. **D.** A trademark is a symbol, word, name, sound, or thing that identifies the origin of a product or service in a particular trade. Answers A, B, and C are incorrect as they do not properly describe a trademark.
12. **A.** Data mining. It is the process of analyzing data to find and understand patterns and relationships about the data. Answers B, C, and D are incorrect. Knowledge management seeks to make intelligent use of all the knowledge in an organization. A data warehouse is a database that contains data from many different databases. Data standards provide consistent meaning to data shared among different information systems.
13. **C.** ISO 27004 is the standard for security management. ISO 27001 is focused on requirements. ISO 27002 was developed from BS 7799, and ISO 27799 is focused on health.
14. **D.** Fiber Channel over Ethernet (FCoE) can operate at speeds of 10 GB per second and rides on top of the Ethernet protocol. While it is fast, it has a disadvantage in that it is non-routable. Answers A, B, and C are incorrect. SCSI is used for local devices only. iSCSI is a SAN standard used for connecting data storage facilities and allowing remote SCSI devices to communicate. HBAs are used to connect a host system to an enterprise storage device.
15. **A.** Some day-to-day responsibility may be passed down to the custodian; however, ultimately the owner is responsible.

Need to Know More?

Data valuation: www.cio.com/article/2375569/cio-role/why-cios-must-own-data-valuation.html

Understanding FIPS guidelines: www.sans.org/reading-room/whitepapers/standards/securing-sensitive-data-understanding-federal-information-processing-standards-fips-549

ISO27002 overview: en.wikipedia.org/wiki/ISO/IEC_27002

Site security: www.faqs.org/rfcs/rfc2196.html

IT asset management: searchcio.techtarget.com/definition/IT-asset-management-information-technology-asset-management

Building effective security policies: www.sans.org/security-resources/policies/

IT security baselines: www.securestate.com/services/minimum-security-baselines

Building effective policy: csrc.nist.gov/nissc/1997/panels/isptg/pescatore/html/

Hard drive disposal: www.semshred.com/contentmgr/showdetails.php/id/2480

This page intentionally left blank

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y

Z