EXAM CRAM

CompTIA® Security+ SY0-301

Third Edition

CD FEATURES TEST QUESTIONS

PEARSON

KIRK HAUSMAN, MARTIN WEISS,
DIANE BARRETT

EXAM CRAM

CompTIA® Security+™ SY0-301

Third Edition

Diane Barrett,
Kalani K. Hausman,
and Martin Weiss

CompTIA Security+™ SY0-301 Authorized Exam Cram, Third Edition

ISBN-13: 978-0-7897-4829-4

ISBN-10: 0-7897-4829-0

Library of Congress Cataloging-in-Publication data is on file.

Printed in the United States of America

Fifth Printing: April 2014

Associate Publisher
David Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Andrew Cupp

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Charlotte Kughen, The Wordsmithery LLC

Indexer
Tim Wright

Proofreader
Megan Wade

Technical Editor
Chris Crayton

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Tim Warner

Book Designer
Gary Adair

Composition
TnT Design, Inc.

Contents at a Glance

Table of Contents

Part II: Compliance and Operational Security

Part IV: Application, Data, and Host Security

Part V: Access Control and Identity Management

About the Authors

Diane Barrett is the director of training for Paraben Corporation and an adjunct professor for American Military University. She has done contract forensic and security assessment work for several years and has authored other security and forensic books. She is a regular committee member for ADFSL's Conference on Digital Forensics, Security, and Law as well as an academy director for Edvancement Solutions. She holds many industry certifications, including CISSP, ISSMP, DFCP, PCME, and Security+. Diane's education includes an MS in information technology with a specialization in information security. She expects to complete a PhD in business administration with a specialization in information security.

Kalani Kirk Hausman is an author, enterprise and security architect, ISO, and consultant with experience including medium- to large-scale globally deployed networks in governmental, higher-education, health-care, and corporate settings. Kalani's professional certifications include the CISSP, CGEIT, CRISC, CISA, CISM, GIAC-GHSC, PMP, and CCP. He is active within the FBI InfraGard, Information Systems Audit and Control Association (ISACA), and ISSA. Kalani is currently employed as the assistant commandant for Strategic Communications, Information Technology, and Public Relations at TAMU and as an adjunct professor of InfoSec at UMUC. Kalani can be reached at kkhausman@hotmail.com or followed on Twitter at @kkhausman.

Martin Weiss lives within a triangle of sales, engineering, and marketing, providing information security solutions for organizations of all sizes. He is currently most interested in governance, risk, compliance, and how to secure elastic cloud environments. He is also an adjunct professor with the University of Maryland University College focusing on security classes. Marty is the author of several other books. His work has been compared to literary greats. His mother, upon reviewing a recent book, described it as riveting as anything by Dostoevsky. Marty holds several certifications, including Security+, CISSP, CISA, and CCSK. He received his M.B.A. from the Isenberg School of Management at the University of Massachusetts and currently lives in Connecticut with his wife, three sons, and iPhone. Marty can be reached at martyweiss@gmail.com or stalked on Twitter @martyweiss.

Dedication

To my husband, Bill, for his patience and understanding.
—Diane Barrett

To Susan and our wonderful children, Jonathan and Cassandra,
who inspire me every moment to greater deeds.
—Kalani K. Hausman

vp,[yos drvitoyu [;id rcs, vts, drvpmf rfoyopm eo;; ntrsl yjr vpfr 2521202 0861704
3330307 3251403
—Martin Weiss

Acknowledgments

Publishing a book takes the collaboration and teamwork of many individuals. Thanks to everyone involved in this process from Waterside Productions and Pearson Education (and thanks to those who purchase this book in their quest for certification). Betsy, thanks for keeping us all on track. To our editorial and technical reviewers, thank you for making sure that our work was sound and on target. Special thanks to my coauthors, Marty and Kirk: You made this project interesting and enjoyable.

—Diane Barrett

Thanks go to my extraordinary agent Carole McClendon, to Betsy Brown, and the Pearson editorial staff. Special thanks go to my coauthors Martin Weiss and Diane Barrett, whose strengths and knowledge produced a remarkable product in this text. As always, the unflagging support of Susan and our wonderful children (Jonathan and Cassandra) was instrumental in completing this book.

—Kalani K. Hausman

Thank you to the entire team that helped bring this book together, including all the folks at Waterside Productions and Pearson. Special thanks to Carole Jelen, Betsy Brown, Andrew Cupp, and, of course, Diane and Kirk. Most importantly I thank you, the reader of this book. Finally, I'd like to acknowledge my family. Thank you to my boys—Ollie, Max, and Kobe; you inspire me. I'm especially thankful to my wife Kelly, who provided a lot of understanding and support during a particularly busy time for me.

—Martin Weiss

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.

As an Associate Publisher for Pearson IT Certification, I welcome your comments. You can email or write me directly to let me 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 I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

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

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
800 East 96th Street
Indianapolis, IN 46240 USA

CompTIA

CompTIA Security+

Designed for IT professionals focused on system security.

Covers network infrastructure, cryptography, assessments, and audits.

Security+ is mandated by the U.S. Department of Defense and is recommended by top companies such as Microsoft, HP, and Cisco.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill— Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly valued credentials that qualify you for jobs, increased compensation and promotion.

Security is one of the highest demand job categories—growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.

CompTIA Security+

Jobs for security administrators are expected to increase by 18%—the skill set required for these types of jobs map to CompTIA Security+ certification.

Network Security Administrators—can earn as much as $106,000 per year.

CompTIA Security+ is the first step—in starting your career as a Network Security Administrator or Systems Security Administrator.

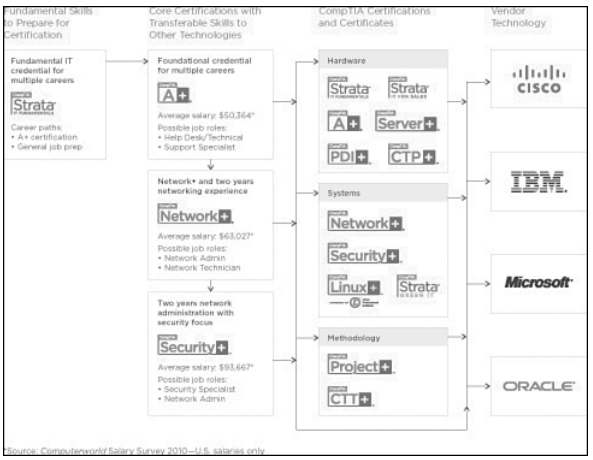
CompTIA Security+ is regularly used in organizations—such as Hitachi Information Systems, Trendmicro, the McAfee Elite Partner program, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

How Certification Helps Your Career

IT Is Everywhere	IT Knowledge and Skills Gets Jobs	Retain Your Job and Salary	Want to Change Jobs	Stick Out from the Resume Pile
IT is ubiquitous, needed by most organizations. Globally, there are over 600,000 IT job openings.	Certifications are essential credentials that qualify you for jobs, increased compensation, and promotion.	Make your expertise stand above the rest. Competence is usually retained during times of change.	Certifications qualify you for new opportunities, whether locked into a current job, see limited advancement, or need to change careers.	Hiring managers can demand the strongest skill set.

CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.



Steps to Getting Certified and Staying Certified	
Review Exam Objectives	Review the certification objectives to make sure you know what is covered in the exam. http://certification.comptia.org/Training/testingcenters/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, take a free assessment and sample test to get an idea of what type of questions might be on the exam. http://certification.comptia.org/Training/testingcenters/samplequestions.aspx
Purchase an Exam Voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at: http://www.comptiastore.com/
Take the Test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: http://certification.comptia.org/Training/testingcenters.aspx
Stay Certified! Continuing education	Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of your certification. There are a number of ways the certification can be renewed. For more information go to: http://certification.comptia.org/getCertified/steps_to_certification/stayCertified.aspx

Join the Professional Community	
Join IT Pro Community http://itpro.comptia.org	The free IT Pro online community provides valuable content to students and professionals. Career IT Job Resources ▶ Where to start in IT ▶ Career Assessments ▶ Salary Trends ▶ US Job Board Forums on Networking, Security, Computing and Cutting Edge Technologies Access to blogs written by Industry Experts Current information on Cutting Edge Technologies Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This courseware bears the seal of **CompTIA Approved Quality Content.** This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

Global Recognition—CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.

Valued by Hiring Managers—Hiring managers value CompTIA certification, because it is vendor- and technology-independent validation of your technical skills.

Recommended or Required by Government and Businesses—Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (For example, Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more.)

Three CompTIA Certifications ranked in the top 10—In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

Visit CompTIA online—www.comptia.org to learn more about getting CompTIA certified.

Contact CompTIA—Call 866-835-8020 ext. 5 or email questions@comptia.org.

Join the IT Pro Community—http://itpro.comptia.org to join the IT community to get relevant career information.

Connect with us— 

Introduction

Welcome to *CompTIA Security+ Exam Cram*, Third Edition. This book aims to help you get ready to take and pass the CompTIA Security+ exam, number SY0-301.

Chapters 1–13 are designed to remind you of everything you need to know to pass the SY0-301 certification exam. The two practice exams at the end of this book should give you a reasonably accurate assessment of your knowledge, and, yes, we've provided the answers and their explanations for these practice exams. Read this book, understand the material, and you'll stand a very good chance of passing the real test.

Exam Cram books help you understand and appreciate the subjects and materials you need to know to pass CompTIA certification exams. *Exam Cram* books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, the authors streamline and highlight the pertinent information by presenting and dissecting the questions and problems they've discovered that you're likely to encounter on a CompTIA test.

We strongly recommend that you spend some time installing, configuring, and working with the latest operating systems to patch and maintain them for the best and most current security possible because the Security+ exam focuses on such activities and the knowledge and skills they can provide for you. Nothing beats hands-on experience and familiarity when it comes to understanding the questions you're likely to encounter on a certification test. Book learning is essential, but, without doubt, hands-on experience is the best teacher of all!

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take the Security+ exam is $266 USD for individuals ($226 for CompTIA members). CompTIA corporate members receive discounts on nonmember pricing. For more information about these discounts, a local CompTIA sales representative can provide answers to any questions you might have. If you don't pass, you can take the exam again for the same cost as the first attempt, for each attempt until you pass. In the United States and Canada, tests are administered by Prometric or VUE.

After you sign up for a test, you are told when and where the test is scheduled. You should arrive at least 15 minutes early. To be admitted into the testing room, you must supply two forms of identification, one of which must be a photo ID.

About This Book

We've structured the topics in this book to build on one another. Therefore, some topics in later chapters make the most sense after you've read earlier chapters. That's why we suggest that you read this book from front to back for your initial test preparation. If you need to brush up on a topic or if you have to bone up for a second try, you can use the index, table of contents, or Table I-1 to go straight to the topics and questions that you need to study. Beyond helping you prepare for the test, we think you'll find this book useful as a tightly focused reference to some of the most important aspects of the Security+ certification.

Chapter Format and Conventions

Every *Exam Cram* chapter follows a standard structure and contains graphical clues about important information. The structure of each chapter includes the following:

- **Opening objectives list:** This defines the official CompTIA Security+ exam objectives covered in the chapter.
- **Cram Saver questions:** Each major section begins with a Cram Saver to help you determine your current level of knowledge of the topics in that section.
- **Topical coverage:** The heart of the chapter. Explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions geared to build your knowledge so that you can pass the exam.
- **Exam Alerts:** These are interspersed throughout the book. They include important information on test topics. Watch out for them!

ExamAlert

This is what an Exam Alert looks like. Normally, an alert stresses concepts, terms, hardware, software, or activities that are likely to relate to one or more certification test questions.

- **Cram Quiz questions:** At the end of each topic is a quiz. The quizzes, and ensuing explanations, are meant to gauge your knowledge of the subjects. If the answers to the questions don't come readily to you, consider reviewing the section.

Additional Elements

Beyond the chapters there are a few more elements:

- **Practice Exams:** There are two practice exams. They are printed in the book and included with the Pearson IT Certification Practice Test Engine on the CD.
- **Cram Sheet:** The tear-out Cram Sheet is located right in the beginning of the book. This is designed to jam some of the most important facts you need to know for the exam into one small sheet, allowing for easy memorization.
- **Glossary:** Definitions of key CompTIA Security+ exam terms.

Exam Objectives

Table I-1 lists the skills measured by the SY0-301 exam and the chapter in which the objective is discussed. Some objectives are covered in other chapters, too.

TABLE I-1 **CompTIA SY0-301 Exam Objectives**

Exam Objective	Chapter
Domain 1: Network Security	
Explain the security function and purpose of network	1
Apply and implement secure network administration principles	1
Distinguish and differentiate network design elements and compounds	1
Implement and use common protocols	2
Identify commonly used default network ports	2
Implement wireless network in a secure manner	2
Domain 2: Compliance and Operational Security	
Explain risk-related concepts	3
Carry out appropriate risk-mitigation strategies	3
Execute appropriate incident response procedures	4
Explain the importance of security-related awareness and training	3
Compare and contrast aspects of business continuity	4
Explain the impact and proper use of environmental controls	4
Execute disaster recovery plans and procedures	4
Exemplify the concepts of confidentiality, integrity, and availability (CIA)	3
Domain 3: Threats and Vulnerabilities	
Analyze and differentiate among types of malware	5
Analyze and differentiate among types of attacks	5
Analyze and differentiate among types of social engineering attacks	5

Exam Objective	Chapter
Domain 3: Threats and Vulnerabilities	
Analyze and differentiate among types of wireless attacks	5
Analyze and differentiate among types of application attacks	5
Analyze and differentiate among types of mitigation and deterrent techniques	6
Implement assessment tools and techniques to discover security threats and vulnerabilities	6
Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning	6
Domain 4: Application, Data, and Host Security	
Explain the importance of application security	7
Carry out appropriate procedures to establish host security	8
Explain the importance of data security	9
Domain 5: Access Control and Identity Management	
Explain the function and purpose of authentication services	10
Explain the fundamental concepts and best practices related to authentication, authorization and access control	10
Implement appropriate security controls when performing account management	11
Domain 6: Cryptography	
Summarize general cryptography concepts	12
Use and apply appropriate cryptographic tools and products	12
Explain the core concepts of public key infrastructure	13
Implement PKI, certificate management, and associated components	13

Pearson IT Certification Practice Test Engine and Questions on the CD

The CD in the back of the book 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 CD in the back of this book has a recent copy of the Pearson IT Certification Practice Test engine. The practice exam—the database of exam questions—is not on the CD.

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

Install the Software from the CD

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 PC platform. The minimum system requirements are the following:

- Windows XP (SP3), Windows Vista (SP2), or Windows 7
- Microsoft .NET Framework 4.0 Client
- Microsoft SQL Server Compact 4.0
- Pentium class 1GHz processor (or equivalent)
- 512MB RAM
- 650MB disc space plus 50MB for each downloaded practice exam

The software installation process is 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 CD sleeve.

The following steps outline the installation process:

1. Insert the CD into your PC.
2. The software that automatically runs is the Pearson software to access and use all CD-based features. From the main menu, click the option to **Install the Exam Engine**.
3. Respond to windows prompts as with any typical software installation process.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the CD sleeve. This process requires that you establish a Pearson website login. You 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

After 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:

1. Start the Pearson IT Certification Practice Test software from the Windows **Start** menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the **My Products** or **Tools** tab, select the **Activate** button.
3. At the next screen, enter the Activation Key from the paper inside the cardboard CD holder in the back of the book. Once entered, click the **Activate** button.
4. The activation process will download the practice exam. Click **Next** and then click **Finish.**

After you've completed the activation process, 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 you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Updating your exams ensures you have the latest changes and updates to the exam data.

If you want 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 ensures 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 Cert Guide or Cisco Press Official Cert Guide, extract the activation code from the CD sleeve in the back of that book—you don't even need the CD at this point. From there, all you have to do is start the exam engine (if it is not still up and running) and perform steps 2–4 from the previous list.

Premium Edition

In addition to the free practice exams provided with your purchase, you can purchase one additional exam with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional full practice exam as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

If you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the CD sleeve that contains a one-time use code as well as instructions for where you can purchase the Premium Edition.

To view the premium edition product page, go to:
http://www.pearsonitcertification.com/store/product.aspx?isbn=0132939592

This page intentionally left blank

CHAPTER 3

Risk Management

This chapter covers the following official CompTIA Security+, SY0-301 exam objectives:

- Exemplify the concepts of confidentiality, integrity, and availability (CIA)
- Explain risk-related concepts
- Carry out appropriate risk mitigation strategies
- Explain the importance of security-related awareness and training

(For more information on the official CompTIA Security+, SY0-301 exam topics, see the "About the CompTIA Security+, SY0-301 Exam" section in the Introduction.)

The traditional "C-I-A Triad" of security directives includes maintaining the confidentiality, integrity, and availability of data and services. Threats to these three principles are constantly present and evolving. Defensive measures must be put into place to mitigate risk within the enterprise. This chapter examines risk, mitigation strategies, and the value of security-awareness training in managing risk.

Exemplify the Concepts of Confidentiality, Integrity, and Availability

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Which element of the C-I-A Triad is addressed by biometric controls?
2. Off-site backup tapes ensure which element of the C-I-A Triad?
3. Battery backup power supplies (UPSs) support which element of the C-I-A Triad?

Answers

1. Confidentiality. Access control mechanisms such as biometric authentication systems ensure that data confidentiality is maintained.
2. Availability. Backup media is used to restore data lost, corrupted, or otherwise at risk of becoming unavailable.
3. Availability. Loss of power prevents services from remaining available to authorized access requests.

Confidentiality

The first principle of information security is that of confidentiality. Confidentiality involves controls to ensure that security is maintained when data is both at rest (stored) and in use (during processing and transport) to protect against unauthorized access or disclosure.

Confidentiality controls include physical access controls, data encryption, logical access controls, and management controls to put in place policies to protect against shoulder surfing, social engineering, and other forms of observational disclosure. We discuss individual access control mechanisms later in this book; this chapter addresses them only in terms of risk mitigation.

ExamAlert

Some questions might include controls that fulfill more than one principle of security, such as access controls that protect both confidentiality and integrity by limiting unauthorized access to examine data (confidentiality) and to modify data (integrity), or malware defenses that protect against key loggers (confidentiality) as well as drive deletion logic bombs (integrity). In these cases, it is best to look for additional details that can reveal the best answer.

Integrity

The second principle of information security is that of integrity. Integrity involves controls to preserve the reliability and accuracy of data and processes against unauthorized modification. Integrity controls include malware defenses protecting against data corruption or elimination, validation code that protects against code injection or malformed data input, data hashing validation identifying modifications, and limited user interface options controlling the types of access available to data.

ExamAlert

Integrity is focused on preserving data against unauthorized modification, which might include deletion, but controls for recovery in the case of deletion might fall more accurately into the Availability arena.

Availability

The final principle of information security is that of availability. Availability involves controls to preserve operations and data in the face of service outages, disaster, or capacity variation. Availability controls include load balancing systems, redundant services and hardware, backup solutions, and environmental controls intended to overcome outages affecting networking, power, system, and service outages.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which two of the following support the preservation of data availability?
   - ❍ **A.** Anti-static carpet
   - ❍ **B.** Firewall
   - ❍ **C.** Mirrored windows
   - ❍ **D.** Physical access control

2. Antivirus software preserves which two elements of data security?
   - ❍ **A.** Confidentiality and Integrity
   - ❍ **B.** Integrity and Availability
   - ❍ **C.** Availability and Confidentiality
   - ❍ **D.** Accuracy and Reliability

3. Regularly expiring passwords preserves data _____ and _____.
   - ❍ **A.** Confidentiality
   - ❍ **B.** Integrity
   - ❍ **C.** Availability
   - ❍ **D.** Longevity

Cram Quiz Answers

1. **A** and **D**. Environmental controls such as anti-static carpeting aid in protecting against system failure and so preserve availability of data and services. Physical access controls protect against system theft, destruction, or damage. Answer B is incorrect because firewalls restrict access data and services, and although deletion is possible, this control is focused on preserving confidentiality and integrity. Answer C is incorrect because mirrored windows protect confidentiality by preventing observation of displayed data, user keystrokes, and other information of potential interest.
2. **A**. Malware defenses such as antivirus services protect the confidentiality and integrity of data by eliminating viral agents that could otherwise capture keystrokes, relay webcam audio/video, or modify data and services. Answers B and C are incorrect because malware defenses are not focused on the preservation of data and service availability beyond preventing outright wipe of the infected system. Answer D is incorrect because accuracy and reliability are data qualities within the Integrity principle, not directly parts of the C-I-A Triad.
3. **A** and **B**. Regular password expiration protects against reuse of compromised passwords and mitigates brute-force attacks by changing keys before all combinations can be tested. These actions protect access controls over data review and modification, preserving confidentiality and integrity of data. Answer C is incorrect because password expiration does not directly affect data and service availability. Similarly, answer D is incorrect because data longevity is unrelated to passwords and exists only as business operations allow. Some data might be updated many times every minute whereas other data remains static for years.

Explain Risk-Related Concepts

- **Control types**
- **False positives**
- **Importance of policies in reducing risk**
- **Risk calculation**
- **Quantitative versus qualitative**
- **Risk-avoidance, transference, acceptance, mitigation, deterrence**
- **Risks associated to cloud computing and virtualization**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. Purchasing an insurance plan to cover the costs of a stolen computer is an example of which risk management strategy?
2. If a risk has an ALE of $25,000 and an ARO of 50%, what is the value of its SLE?
3. What are the three categories commonly used to identify the likelihood of a risk?

Answers

1. Transference. The costs if the risk is actualized are transferred to the insurance company. The risk, however, is not reduced; only its cost effect has been transferred, and other issues, such as client loss of trust, might produce second-order effects.
2. The single loss expectancy (SLE) is $50,000 per event. With an annualize rate of occurrence (ARO) of 50%, this risk is expected to occur once every other year on average, so the annualized loss expectancy (ALE) is equal to the SLE ($50,000) times the ARO (.5) or $25,000.
3. Likelihood is commonly assigned as High (1.0), Medium (0.5), or Low (0.1) values for risk comparison.

Risk Responses

Risk management deals with the alignment of five potential responses with an identified risk:

- **Acceptance:** Recognizing a risk, identifying it, and then accepting that it is sufficiently unlikely or of such limited impact that corrective controls

are not warranted. Risk acceptance must be a conscious choice, documented, approved by senior administration, and regularly reviewed.

- **Avoidance:** Elimination of the vulnerability that gives rise to a particular risk so that it is avoided altogether. This is the most effective solution, but often not possible due to organizational requirements. Eliminating email to avoid the risk of email-borne viruses is an effective solution but not likely to be a realistic approach in the modern enterprise.
- **Mitigation/Deterrence:** Risk mitigation involves the reduction in likelihood or impact of a risk's exposure. Risk deterrence involves putting into place systems and policies to mitigate a risk by protecting against the exploitation of vulnerabilities that cannot be eliminated. Most risk management decisions focus on mitigation and deterrence, balancing costs and resources against the level of risk and mitigation that will result.
- **Transference:** A risk or the effect of its exposure may be transferred by moving to hosted providers who assume the responsibility for recovery and restoration or by acquiring insurance to cover the costs emerging from equipment theft or data exposure.

ExamAlert

Risk management employs several terms that you should familiarize yourself with before the exam:

- **Vulnerability:** A vulnerability is a weakness in hardware, software, process, or people that can be employed or engaged to affect enterprise security.
- **Exploit:** An exploit is a mechanism of taking advantage of an identified vulnerability.
- **Threat:** A threat is the potential that a vulnerability will be identified and exploited.
- **Risk:** A risk is the likelihood that a threat will occur and the measure of its effect.
- **Control:** Controls act to close vulnerabilities, prevent exploitation, reduce threat potential, and/or reduce the likelihood of a risk or its impact.

Types of Controls

You can apply three general types of controls to mitigate risks, typically by layering defensive controls to protect data with multiple control types when possible. This technique is called a layered defensive strategy or "defense in depth."

The three types of controls include the following:

- **Management:** Management or administrative controls include business and organizational processes and procedures, such as security policies and procedures, personnel background checks, security awareness training, and formal change-management procedures.
- **Technical:** Technical controls include logical access control systems, security systems, encryption, and data classification solutions.
- **Operational:** Operational controls include organizational culture as well as physical controls that form the outer line of defense against direct access to data, such as protection of backup media; securing output and mobile file storage devices; and facility design details including layout, doors, guards, locks, and surveillance systems.

ExamAlert

Controls are intended to mitigate risk in some manner, but at times they might fail in operation. You should be familiar with the following terms for the exam:

- **False Positive:** A control that allows unauthorized access, falsely identifying the access as valid.
- **False Negative:** A control that refuses authorized access, falsely identifying the access as invalid.

Identifying Vulnerabilities

Many risks to enterprise networks relate to vulnerabilities present in system and service configurations and to network and user logon weaknesses. For the exam, you should be familiar with some of the more common tools used to conduct vulnerability assessments, including the following:

- **Port scanners:** This software utility scans a single machine or a range of IP addresses, checking for a response on service ports. A response on port 80, for example, might reveal the operation of an HTTP host. Port scanners are useful in creating an inventory of services hosted on networked systems. When applied to test ports on a single system, this is termed a *port scan*, whereas a scan across multiple hosts is referred to as a *port sweep*.
- **Vulnerability scanners:** This software utility scans a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services. Unlike port scanners, which only

test for the availability of services, vulnerability scanners may check for the particular version or patch level of a service to determine its level of vulnerability.

- **Protocol analyzers:** This software utility is used on a hub, a switch supervisory port, or in line with network connectivity to enable the analysis of network communications. Individual protocols, specific endpoints, or sequential access attempts can be identified using this utility, which is often referred to as a *packet sniffer*.
- **Network mappers:** Another software utility used to conduct network assessments over a range of IP addresses, the network mapper compiles a listing of all systems, devices, and network hardware present within a network segment. This information can be used to identify simple points of failure, to conduct a network inventory, and to create graphical details suitable for reporting on network configurations.
- **Password crackers:** This software utility allows direct testing of user logon password strength by conducting a brute-force password test using dictionary terms, specialized lexicons, or mandatory complexity guidelines. Password crackers should provide only the relative strength of a password, rather than the password itself, to avoid weakening logon responsibility under evidentiary discovery actions.

Identifying Risk

Risk is the possibility of loss or danger. Risk management is the process of identifying and reducing risk to a level that is comfortable and then implementing controls to maintain that level. Risk analysis helps align security objectives with business objectives. Here, we deal with how to calculate risk and return on investment. Risk comes in a variety of forms. Risk analysis identifies risks, estimates the effect of potential threats, and identifies ways to reduce the risk without the cost of the prevention outweighing the risk.

Measuring Risk

The annual cost of prevention against threats is compared to the expected cost of loss—a cost/benefit comparison. To calculate costs and return on investment, you must first identify your assets, the threats to your network, your vulnerabilities, and what risks result. For example, a virus is a threat; the vulnerability would be not having antivirus software; and the resulting risk would be the effects of a virus infection. All risks have loss potential. Because security

resources will always be limited in some manner, it is important to determine what resources are present that may need securing. Then, you need to determine the threat level of exposure that each resource creates and plan your network defenses accordingly.

Asset Identification

Before you can determine which resources are most in need of protection, it is important to properly document all available resources. A resource can refer to a physical item (such as a server or piece of networking equipment), a logical object (such as a website or financial report), or even a business procedure (such as a distribution strategy or marketing scheme). Sales demographics, trade secrets, customer data, and even payroll information could be considered sensitive resources within an organization. When evaluating assets, consider the following factors:

- The original cost
- The replacement cost
- Its worth to the competition
- Its value to the organization
- Maintenance costs
- The amount it generates in profit

After you have identified and valued assets, an appropriate dollar amount can be spent to help protect those assets from loss.

The Risk and Threat Assessment

After assets have been identified, you must determine the assets' order of importance and which assets pose significant security risks. During the process of risk assessment, it is necessary to review many areas, such as the following:

- Methods of access
- Authentication schemes
- Audit policies
- Hiring and release procedures
- Isolated and non-redundant systems and services that may provide a single point of failure or avenue of compromise
- Data or services requiring special backup or automatic failover support

Risk assessment should include planning against both external and internal threats. An insider familiar with an organization's procedures can pose a very dangerous risk to network security.

During a risk assessment, it is important to identify potential threats and document standard response policies for each. Threats may include the following:

- Direct access attempts
- Automated cracking agents
- Viral agents, including worms and Trojan horses
- Released or dissatisfied employees
- Denial-of-service (DoS) attacks or overloaded capacity on critical services
- Hardware or software failure, including facility-related issues such as power or plumbing failures

Likelihood

When examining threat assessment, you have to consider the likelihood that the threats you've identified might actually occur. To gauge the probability of an event occurring as accurately as possible, you can use a combination of estimation and historical data. Most risk analyses use a fiscal year to set a time limit of probability and confine proposed expenditures, budget, and depreciation.

The National Institute of Standards and Technology (NIST) 800.30 document suggests measuring likelihood as High, Medium, or Low based on the motivation and capability of the threat source, the nature of the vulnerability, and the existence and effectiveness of current controls to mitigate the threat. Often the three values are translated into numerical equivalents for use in quantitative analytical processes: High (1.0), Medium (0.5), Low (0.1).

Responses must be coupled to the likelihood determined in the risk analysis, such as identifying the need to put corrective measures in place as soon as possible for all High-level threats, whereas Medium-level threats might only require an action plan for implementation as soon as is reasonable, and Low-level threats might be dealt with as possible or simply accepted.

Calculating Risk

To calculate risk, use this formula:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

To help you understand this, let's look at an example using DoS attacks. Firewall logs indicate that the organization was hit hard one time per month by a DoS attack in each of the past six months. You can use this historical data to estimate that it's likely you will be hit 12 times per year. This information helps you calculate the single loss expectancy (SLE) and the annual loss expectancy (ALE).

SLE equals asset value multiplied by the threat exposure factor or probability. The formula looks like this:

Asset value × Probability = SLE

The exposure factor or probability is the percentage of loss that a realized threat could have on a certain asset. In the DoS example, let's say that if a DoS were successful, 25% of business would be lost. The daily sales from the website are $100,000, so the SLE would be $25,000 (SLE = $100,000 × .25). The possibility of certain threats is greater than that of others. Historical data presents the best method of estimating these possibilities.

After you calculate the SLE, you can calculate the ALE. This gives you the probability of an event happening over a single year's time. This is done by calculating the product of the SLE and the value of the asset. ALE equals the SLE times the ARO (annualized rate of occurrence):

SLE × ARO = ALE

The ARO is the estimated possibility of a specific threat taking place in a one-year time frame. When the probability that a DoS attack will occur is 50%, the ARO is 0.5. Going back to the example, if the SLE is estimated at $25,000 and the ARO is .5, our ALE is 12,500. ($25,000 × .5 = $12,500). Spending more than $12,500 might not be prudent because the cost would outweigh the risk.

ExamAlert

Other risk models for calculating risk include the cumulative loss expectancy (CLE) and Iowa risk model. The cumulative loss expectancy (CLE) model calculates risk based on single systems. It takes into account all the threats that are likely to happen to this system over the next year, such as natural disasters, malicious code outbreak, sabotage, and backup failure. The Iowa risk model determines risk based on criticality and vulnerability.

Calculating Reduced Risk on Investment

Return on investment is the ratio of money realized or unrealized on an investment relative to the amount of money invested. Because there are so many vulnerabilities to consider and so many different technologies available, calculating

the ROI for security spending can prove difficult. The formulas present too many unknowns. Many organizations don't know how many actual security incidents have occurred, nor have they tracked the cost associated with them.

One method that might be helpful in this area is called *reduced risk on investment (RROI)*. This method enables you to rank security investments based on the amount of risk they reduce. Risk is calculated by multiplying potential loss by the probability of an incident happening and dividing the result by the total expense:

RROI = Potential loss × (Probability without expense – Probability with expense) / Total expense

By using this formula, you can base alternative security investments on their projected business value.

Another approach is to look at security as loss prevention. It can be equated to loss prevention in that attacks can be prevented. ROI is calculated using the following formula:

ROI = Loss prevented – Cost of solution

If the result of this formula is a negative number, you spent more than the loss prevented.

Qualitative versus Quantitative Measures

Quantitative measures allow for the clearest measure of relative risk and expected return on investment or risk reduction on investment. Not all risk can be measured quantitatively, though, requiring qualitative risk assessment strategies. The culture of an organization greatly affects whether its risk assessments can be performed via quantitative (numerical) or qualitative (subjective/relative) measures.

Qualitative risk assessment can involve brainstorming, focus groups, surveys, and other similar processes to determine asset worth and valuation to the organization. Uncertainty is also estimated, allowing for a relative projection of qualitative risk for each threat based on its position in a risk matrix plotting the Probability (Low to High) and Impact (Low to High) of each. It is possible to assign numerical values to each state (Very Low = 1, Low = 2, Moderate = 3, and so on) so that a quasi-quantitative analysis can be performed, but because the categories are subjectively assigned, the result remains a qualitative measure.

Quantitative measures tend to be more difficult for management to understand, require very intensive labor to gather all related measurements, and are more time consuming to determine. Qualitative measures tend to be less precise, more subjective, and difficult to assign direct costs for measuring ROI/RROI.

ExamAlert

Because risks within cloud and virtualized hosting systems require knowledge of location, host system, shared tenancy, and other operational details subject to regular and ongoing change as data is migrated within the hosting environment, risk assessment of these environments depends on subjective assessment and service-level contractual expectations. The subjective and uncertain nature of assessments within these environments falls into the qualitative form of risk assessment.

Cloud computing solutions except for a private cloud (meaning both public and hybrid clouds) encompass all of the normal concerns of enterprise resources, together with those for outsourced resources. And because cloud computing is built atop virtualized computing models, the same factors apply to virtualized as well as cloud-based computing systems and services.

These considerations include the following:

- **Secure data transfer:** Because data must travel over public Internet connections for both hosted and hybrid clouds, data must be encrypted and authenticated between endpoints.
- **Secure APIs:** Application interfaces must be protected against unauthorized access as well as flood attacks intended to deny legitimate access to remote resources.
- **Secure data storage:** Data must be encrypted at rest and in backup media to protect against unauthorized access even with physical server access.
- **User access controls:** Logging and audit provisions for all access should be implemented to ensure that all access, both organizational and host-side, is limited to authorized requests.
- **Data separation:** Shared hosting creates the potential for resource competition on the host server and its network connections. Compartmentalization of data storage and service function may also be mandated by regulatory directives in some industries.

Risk Reduction Policies

To ensure that proper risk management and incident response planning is coordinated, updated, communicated, and maintained, it is important to establish clear and detailed security policies that are ratified by an organization's management and brought to the attention of its users through regular security-awareness

training. Policies of which the users have no knowledge are rarely effective, and those that lack management support can prove to be unenforceable.

A number of policies support risk-management practices within the enterprise, including the following:

- Privacy
- Acceptable use
- Storage and retention
- Secure disposal
- Account provisioning
- Least privilege
- Separation of duties
- Mandatory vacations
- Job rotation

Privacy

Privacy-sensitive information is referred to as *personally identifiable information (PII)*. This is any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. Examples of PII are name, address, phone number, fax number, email address, financial profiles, Social Security number, and credit card information. For many organizations, privacy policies are mandatory, have detailed requirements, and carry significant legal penalties (for example, entities covered under the Health Insurance Privacy and Portability Act).

To be considered PII, information must be specifically associated with an individual person. Information provided either anonymously or not associated with its owner before collection is not considered PII. Unique information, such as a personal profile, unique identifier, biometric information, and IP address that is associated with PII, can also be considered PII.

The California Online Privacy Protection Act of 2003 (OPPA), which became effective on July 1, 2004, requires owners of commercial websites or online services to post a privacy policy. OPPA requires that each operator of a commercial website conspicuously post a privacy policy on its website. The privacy policy itself must contain the following features:

- A list of the categories of PII the operator collects

- A list of the categories of third parties with whom the operator might share such PII
- A description of the process by which the consumer can review and request changes to his or her PII collected by the operator
- A description of the process by which the operator notifies consumers of material changes to the operator's privacy policy
- The effective date of the privacy policy

Other federal and state laws might apply to PII. In addition, other countries have laws as to what information can be collected and stored by organizations. As with most of the information in this chapter, it is imperative that you know the regulations that govern the digital terrain in which your organization operates. The organization then has an obligation to put proper policies and procedures in place.

Acceptable Use

An organization's acceptable use policy must provide details that specify what users may do with their network access. This includes email and instant messaging usage for personal purposes, limitations on access times, and the storage space available to each user. It is important to provide users the least possible access rights while allowing them to fulfill legitimate actions.

An acceptable use policy should contain these main components:

- Clear, specific language
- Detailed standards of behavior
- Detailed enforcement guidelines and standards
- Outline of acceptable and not acceptable uses
- Consent forms
- Privacy statement
- Disclaimer of liability

The organization should be sure the acceptable use policy complies with current state and federal legislation and does not create unnecessary business risk to the company by employee misuse of resources. Upon logon, show a statement to the effect that network access is granted under certain conditions and that all activities may be monitored. This way you can be sure that any legal ramifications are covered.

Storage and Retention

Retention and storage documentation should outline the standards for storing each classification level of data. Take, for example, the military levels of data classification used in their mandatory access control strategy (MAC). Here, documentation would include directions and requirements for handling and storing the following types of data:

- Unclassified
- Sensitive
- Confidential
- Secret
- Top secret

Policies for data should include how to classify, handle, store, and destroy it. The important point to remember here is to document your security objectives. Then, change and adjust that policy when and as needed. There might be a reason to make new classifications as business goals change, but make sure this gets into your documentation. This is an ongoing, ever-changing process.

Log files, physical records, security evaluations, and other operational documentation should be managed within an organization's retention and disposal policies. These should include specifications for access authorization, term of retention, and requirements for disposal. Depending on the relative level of data sensitivity, retention and disposal requirements can become extensive and detailed.

The organization should have a legal hold policy in place, have an understanding of statutory and regulatory document retention requirements, understand the varying statutes of limitations, and maintain a records-retention and destruction schedule.

Secure Disposal

ISO 17799, particularly sections 7 and 8, has established standards for dealing with the proper disposal of obsolete hardware. Standards dictate that equipment owned or used by the organization should be disposed of only in accordance with approved procedures, including independent verification that the relevant security risks have been mitigated. This policy addresses issues that you should consider when disposing of old computer hardware, for recycle, disposal, donation, or resale.

The most prominent example of a security risk involved is that the hard disk inside the computer has not been completely or properly wiped. There are some concerns about data erasure sufficiency in new solid-state drives (SSDs) that might require organizations to totally destroy drivers rather than simply erasing them for normal disposal channels.

When implementing a policy on the secure disposal of outdated equipment, you need to consider a wide range of scenarios, such as the following:

- Breaches of health and safety requirements.
- Inadequate disposal planning results in severe business loss.
- Remnants of legacy data from old systems might still be accessible.
- Disposal of old equipment that is necessary to read archived data.
- Theft of equipment in use during clean-up of unwanted equipment.

Besides properly disposing of old hardware, removable media disposal is just as important. There is a proper way to handle removable media when either the data should be overwritten or is no longer useful or pertinent to the organization.

The following methods are acceptable to use for some forms of media sanitation:

- **Declassification:** A formal process of assessing the risk involved in discarding particular information.
- **Sanitization:** The process of removing the contents from the media as fully as possible, making it extremely difficult to restore.
- **Degaussing:** This method uses an electrical device to reduce the magnetic flux density of the storage media to zero.
- **Overwriting:** This method is applicable to magnetic storage devices.
- **Destruction:** The process of physically destroying the media and the information stored on it. For flash drives and other solid-state non-ferric removable storage, this might prove to be the only solution acceptable under certain controls and legal mandates.

Data Labeling, Handling, and Disposal

An organization's information sensitivity policy defines requirements for the classification and security of data and hardware resources based on their relative level of sensitivity. Some resources, such as hard drives, might require

very extensive preparations before they can be discarded. Data labeling and cataloguing of information stored on each storage device, tape, or removable storage system becomes critical to identifying valuable and sensitive information requiring special handling.

Organizational data assets might also fall under legal discovery mandates, so a careful accounting is vital to ensure that data can be located if requested and is protected against destruction or recycling if it must be provided at a later time. Proper labeling also ensures that data storage media can be properly processed for reuse or disposal, where special requirements for sensitive data might require outright destruction of the storage device and logging of its destruction in the inventory catalog.

Account Provisioning

Human resources (HR) policies and practices should reduce the risk of theft, fraud, or misuse of information facilities by employees, contractors, and third-party users. The primary legal and HR representatives should review all policies, especially privacy issues, legal issues, and HR enforcement language. Legal and HR review of policies is required in many, if not most, organizations.

Security planning must include procedures for the creation and authorization of accounts (provisioning) for newly hired personnel and the planned removal of privileges (de-provisioning) following employment termination. When termination involves power users with high-level access rights or knowledge of service administrator passwords, it is critical to institute password and security updates to exclude known avenues of access while also increasing security monitoring for possible reprisals against the organization.

The hiring process should also include provisions for making new employees aware of acceptable use and disposal policies and the sanctions that might be enacted if violations occur. An organization should also institute a formal code of ethics to which all employees should subscribe, particularly power users with broad administrative rights.

Least Privilege

Policies addressing access rights for user accounts must mandate that only the minimum permissions necessary to perform work should be assigned to a user. This protects against unauthorized internal review of information as well as protecting against inadvertently enacted viral agents running with elevated permissions.

Separation of Duties

Too much power can lead to corruption, whether it is in politics or network administration. Most governments and other organizations implement some type of a balance of power through a separation of duties. It is important to include a separation of duties when planning for security policy compliance. Without this separation, all areas of control and compliance may be left in the hands of a single individual. The idea of separation of duties hinges on the concept that multiple people conspiring to corrupt a system is less likely than a single person corrupting it. Often, you will find this in financial institutions, where to violate the security controls all the participants in the process have to agree to compromise the system.

ExamAlert

For physical or operational security questions, avoid having one individual who has complete control of a transaction or process from beginning to end and implement policies such as job rotation, mandatory vacations, and cross-training. These practices also protect against the loss of a critical skill set due to injury, death, or another form of personnel separation.

Mandatory Vacations and Job Rotation

Users should be required to take mandatory vacations and rotate positions or functional duties as part of the organization's security policy. These policies outline the manner in which a user is associated with necessary information and system resources and that access is rotated between individuals. There must be other employees who can do the job of each employee so that corruption does not occur, cross-checks can be validated, and the effect of personnel loss is minimized. It is imperative that all employees are adequately cross-trained and only have the level of access necessary to perform normal duties (least privilege).

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. A risk has the following calculated values (SLE = $1,500, ARO = 5). What is the maximum amount that should be spent to fully mitigate the costs of this risk?

   - ❍ **A.** $300
   - ❍ **B.** $500
   - ❍ **C.** $1,500
   - ❍ **D.** $7,500

2. Regarding qualitative versus quantitative measures, which of the following statements is true?
   - ❍ **A.** Quantitative measures evaluate risk based on a subjective assessment.
   - ❍ **B.** Qualitative measures are less precise.
   - ❍ **C.** Qualitative measures are easier to measure for ROI/RROI.
   - ❍ **D.** Quantitative measures are always better than qualitative measures.

3. If a risk has the following measures (Asset value = $50, Probability = 10%, ARO = 100), and the mitigation costs $100 per year, what is the expected ROI?
   - ❍ **A.** $400
   - ❍ **B.** $500
   - ❍ **C.** $600
   - ❍ **D.** $700

4. What is the likelihood of a risk requiring corrective actions planned for implementation in a reasonable period of time?
   - ❍ **A.** Very High
   - ❍ **B.** High
   - ❍ **C.** Medium
   - ❍ **D.** Low

Cram Quiz Answers

1. **D**. The ALE = SLE ($1,500) × ARO (5) = $7,500. Spending more than $7,500 to mitigate the threat without other cause such as a regulatory or legal mandate would be without return. Answers A, B, and C present too low a figure and are all incorrect.
2. **B**. Because qualitative measures are based on subjective values, they are less precise than quantitative measures. Answer A is incorrect because quantitative measures rely on numerical values rather than subjective ones. Answer C is incorrect because qualitative measures are harder to assign numerical values and so more difficult to determine ROI. Answer D is incorrect because each form of analysis has its own benefits and neither is always better in all situations than the other.
3. **A**. The single loss expectancy (SLE) can be calculated as the product of the asset value ($50) times the probability of loss (.1) or SLE=$5/year. The annualized rate of occurrence (ARO) is 100 times per year, so the annualized loss expectancy (ALE) is SLE ($5) times the ARO (100) or ALE=$500/year. Because the cost of mitigation is $100 per year, the ROI is equal to the loss prevented (ALE = $500) less the cost of the solution ($100) or ROI = $400. Answers B, C, and D all present potential values higher than $400 and are incorrect.

4. **C**. A Medium-level risk likelihood warrants implementation of controls as soon as is reasonable. Answer A is incorrect because variations between High and Very High are not based on recognized standards such as the NIST 800.30 and instead reflect categories assigned within an organization based on its own criteria. Answer B is incorrect because High-level threats should be corrected as soon as possible, whereas Low-level threats can be dealt with when time allows or be simply accepted, making answer D incorrect as well.

Carry Out Appropriate Risk-Mitigation Strategies

- **Implement security controls based on risk**
- **Change management**
- **Incident management**
- **User rights and permissions reviews**
- **Perform routine audits**
- **Implement policies and procedures to prevent data loss or theft**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. What is the name of the process of removing the contents from media as fully as possible?
2. What is the first step to developing an audit plan for your organization?
3. What two functions should be reviewed during a user access and rights audit?

Answers

1. Sanitization. The fully cleared media is extremely difficult if not impossible to restore.
2. Identification of resources at risk must occur before auditing of controls is possible. Resources include data and services such as sensitive files, financial applications, and personnel files.
3. Both user privilege and usage should be monitored to ensure that access controls are working properly.

As discussed earlier in this chapter, alignment between security controls, policies, and the risks they mitigate requires an assessment of relative risks and the costs associated with mitigation strategies for each. You must put controls in place based on the relative impact of each risk, with legal mandates considered absolute requirements unless designated as "addressable" and properly documented as part of the risk management plan. You should also formulate organizational policies to include change- and incident-management guidelines as well as audit review expectations.

Change Management

You should document all configuration changes. Many companies are lacking in this area. We are often in a hurry to make changes and say we will do the documentation later—most of the time, that doesn't happen. You should realize that documentation is critical. It eliminates misunderstandings and serves as a trail if something goes wrong down the road. Change documentation should include the following:

- Specific details, such as the files being replaced, the configuration being changed, the machines or operating systems affected, and so on
- The name of the authority who approved the changes
- A list of the departments that are involved in performing the changes and the names of the supervisors in those departments
- What the immediate effect of the change will be
- What the long-term effect of the change will be
- The date and time the change will occur

After the change has occurred, the following should be added to the documentation:

- Specific problems and issues that occurred during the process
- Any known workarounds if issues have occurred
- Recommendations and notes on the event

After the change has been requested, documented, and approved, you should then send out notification to the users so that they know what to expect when the change has been implemented.

Incident Management

Incidents do happen from time to time in most organizations no matter how strict security policies and procedures are. It is important to realize that proper incident handling is just as vital as the planning stage, and its presence may make the difference between being able to recover quickly and ruining a business and damaging customer relations. Customers need to see that the company has enough expertise to deal with the problem.

Incident response guidelines, change-management procedures, security procedures, and many other security-related factors require extensive planning and

documentation. Incident response documentation should include the identification of required forensic and data-gathering procedures and proper reporting and recovery procedures for each type of security-related incident.

The components of an incidence-response plan should include preparation, roles, rules, and procedures. Incident-response procedures should define how to maintain business continuity while defending against further attacks. Although many organizations have an incident response team (IRT), which is a specific group of technical and security investigators that respond to and investigate security incidents, many do not. In the event there is no IRT, first responders need to handle the scene and the response. Systems should be secured to prevent as many incidents as possible and monitored to detect security breaches as they occur. The National Institute of Standards and Technology (NIST) has issued a report on incident response guidelines that can help an organization spell out its own internal procedures.

First Responders

First responders are the first ones to arrive at the incident scene. The success of data recovery and potential prosecution depends on the actions of the individual who initially discovers a computer incident. How the evidence scene is handled can severely affect the ability of the organization to prosecute if need be.

Damage and Loss Control

After the response team has determined that an incident occurred, the next step in incident analysis involves taking a comprehensive look at the incident activity to determine the scope, priority, and threat of the incident. This aids with researching possible response and mitigation strategies. In keeping with the severity of the incident, the organization can act to mitigate the effect of the incident by containing it and eventually restoring operations back to normal.

Depending on the severity of the incident and the organizational policy, incident response functions can take many forms. The response team may send out recommendations for recovery, containment, and prevention to systems and network administrators at sites who then complete the response steps. The team may perform the remediation actions themselves. The follow-up response can involve sharing information and lessons learned with other response teams and other appropriate organizations and sites.

After the incident is appropriately handled, the organization might issue a report that details the cause of the incident, the cost of the incident, and the steps the organization should take to prevent future incidents.

It is important to accurately determine the cause of each incident so that it can be fully contained and the exploited vulnerabilities can be mitigated to prevent similar incidents from occurring in the future.

Regular Audits

How much you should audit depends on how much information you want to store. Keep in mind that auditing should be a clear-cut plan built around goals and policies. Without proper planning and policies, you probably will quickly fill your log files and hard drives with useless or unused information.

The more quickly you fill up your log files, the more frequently you need to check the logs; otherwise, important security events might be deleted unnoticed.

Audit Policy

Here are some items to consider when you are ready to implement an audit policy:

- Identify potential resources at risk within your networking environment. These resources might typically include sensitive files, financial applications, and personnel files.
- After the resources are identified, set up the audit policy through the operating system tools. Each operating system will have its own method for tracking and logging access.
- Auditing can easily add an additional 25% load or more on a server. If the policy incorporates auditing large amounts of data, be sure that the hardware has the additional space needed and processing power and memory.

After you have auditing turned on, log files are generated. Schedule regular time to view the logs.

User Access and Rights Review

After you have established the proper access control scheme, it is important to monitor changes in access rights. Auditing user privileges is generally a two-step process that involves turning auditing on within the operating system and then specifying the resources to be audited. After enabling auditing, you also need to monitor the logs that are generated. Auditing should include both privilege and usage. Auditing of access use and rights changes should be implemented to prevent unauthorized or unintentional access or escalation of

privileges, which might allow a guest or restricted user account access to sensitive or protected resources.

Some of the user activities that can be audited include the following:

- Reading, modifying, or deleting files
- Logging on or off the network
- Using services such as remote access or terminal services
- Using devices such as printers

When configuring an audit policy, it is important to monitor successful and failed access attempts. Failure events enable you to identify unauthorized access attempts; successful events can reveal an accidental or intentional escalation of access rights.

ExamAlert

The roles of the computers also determine which events or processes you need to audit and log. For example, auditing a developer's computer might include auditing process tracking, whereas auditing a desktop computer might include auditing directory services access. To audit objects on a member server or a workstation, turn on the audit object access. To audit objects on a domain controller, turn on the audit directory service access. Do not audit the use of user rights unless it is strictly necessary for your environment. If you must audit the use of user rights, it is advisable to purchase or write an event-analysis tool that can filter only the user rights of interest to you. The following user rights are never audited mainly because they are used by processes. However, the assignment of them might be monitored

- Bypass traverse checking
- Generate security audits
- Create a token object
- Debug programs
- Replace a process-level token

System and Service Audits

In addition to auditing events on domain controllers and user computers, servers that perform specific roles, such as a DNS, DHCP, SQL, or Exchange server, should have certain events audited. For example, you should enable audit logging for DHCP servers on your network and check the log files for an unusually high number of lease requests from clients. DHCP servers running Windows Server 2008 include several logging features and server parameters that provide enhanced auditing capabilities, such as specifying the following:

- The directory path in which the DHCP server stores audit log files. By default, the DHCP audit logs are located in the %windir%\System32\Dhcp directory.
- A minimum and maximum size for the total amount of disk space that is available for audit log files created by the DHCP service.
- A disk-checking interval that determines how many times the DHCP server writes audit log events to the log file before checking for available disk space on the server.

Turning on all possible audit counters for all objects could significantly affect server performance, so plan your audit settings and test them regularly.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which policy details what users may do with their network access?
   - ❍ **A.** Privacy
   - ❍ **B.** Acceptable Use
   - ❍ **C.** Storage and Retention
   - ❍ **D.** Secure Disposal

2. When preparing to securely dispose of a hard drive, what is the term for reducing the magnetic flux density of the media to zero?
   - ❍ **A.** Declassification
   - ❍ **B.** Destruction
   - ❍ **C.** Degaussing
   - ❍ **D.** Overwriting

3. The policy preventing too much power leading to corruption is called the _____ policy.
   - ❍ **A.** Account Provisioning
   - ❍ **B.** Least Privilege
   - ❍ **C.** Separation of Duties
   - ❍ **D.** Acceptable Use

Cram Quiz Answers

1. **B**. The Acceptable Use policy details what users may do with their network access, which generally excludes illegal acts and actions that cost the organization money or public favor. Answer A is incorrect as the Privacy policy covers PII protection requirements and practices. Both C and D deal with information storage and storage device disposal so are not related to network access use.
2. **C**. Degaussing involves exposing the media to a powerful electromagnetic device, erasing all magnetic variation within the media. Answer A is incorrect because declassification is a formal process for assessing the risk involved with discarding information, rather than media sanitization itself. Answer B is incorrect because destruction involves physical destruction of the storage device rather than only magnetic degaussing. Answer D is incorrect because overwriting involves the sequential writing of 1s and 0s to mask previously stored data and does not reduce all magnetic flux in the media to zero.
3. **C**. The separation of duties policy ensures that a single individual is not responsible for all areas of control and compliance over an organizational function, which ensures that proper checks and balances remain in effect. Answer A is incorrect because the account provisioning policy details new account-creation protocols, and answer B is incorrect because the principle of least privilege ensures only that permissions are only sufficient for job requirements without precluding assignment of both control and compliance functions to the same individual. Answer D is incorrect because the acceptable use policy defines only what a user may do with his network access, not what roles he may fulfill.

Explain the Importance of Security-Related Awareness and Training

- **Security policy training and procedures**
- **Personally identifiable information**
- **Information classification: sensitivity of data (hard or soft)**
- **Data labeling, handling, and disposal**
- **Compliance with laws, best practices, and standards**
- **User habits**
- **Threat awareness**
- **Use of social networking and P2P**

CramSaver

If you can correctly answer these questions before going through this section, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section.

1. An email to ALLSTAFF detailing a new email virus improves what aspect of user security awareness?
2. When a user switches between organizational sections, what type of security training does he or she need to cover encryption and using USB thumb drives?

Answers

1. Threat awareness. Threat awareness includes recognizing attacks and requires constant reminders of newly emergent threat agents to remain current.
2. Data handling. Because the policies, procedures, and types of data managed in each organizational section can vary widely, it is important to provide a transferring organizational member with data handling training to ensure her compliance with appropriate protocols ad procedures.

One of the most powerful tools available to a security administrator is the body of network users, who might notice and draw attention to unusual access methods or unexpected changes. This same body of users also creates the greatest number of potential security holes because each user might be unaware of newly emerging vulnerabilities, threats, or required standards of

action and access that must be followed. Like a chain, a network is only as secure as its weakest link—and users present a wide variety of bad habits, a vast range of knowledge, and varying intent in access.

User Education

User education is mandatory to ensure that users are made aware of expectations, options, and requirements related to secure access within an organization's network. Education can include many different forms of communication, including the following:

- New employees and contract agents should be provided education in security requirements as a part of the hiring process.
- Reminders and security-awareness newsletters, emails, and flyers should be provided to raise general security awareness.
- General security policies must be defined, documented, and distributed to employees.
- Regular focus group sessions and on-the-job training should be provided for users regarding changes to the user interface, application suites, and general policies.
- General online security-related resources should be made available to users through a simple, concise, and easily navigable interface.

Exam Alert

Although all the previously mentioned practices are part of a security-awareness training program, security training during employee orientation combined with yearly seminars is the best choice, as these are active methods of raising security awareness. Email and posters are passive and tend to be less effective.

User training should ensure that operational guidelines, disaster recovery strategies, and operational mandates are clearly conveyed to users and refreshed regularly. Policies may also require refresher training during transfer between organizational components or job duties under the rotation policy. Details such as information classification, sensitivity of data and handling guidelines, legal mandates, best practices, and standards can vary widely between organizational units with the proper protocols for access, storage, and disposal varying accordingly.

User Habits and Expectations

Security awareness training is also key to managing user habits and expectations developed due to the prevalence of computing equipment at home and in their mobile devices.

Passwords

Users must be instructed in the value of their access credentials and the impact that could result from sharing their passwords and logons, using weak passwords (and the ability to identify a strong password), easily guessed passwords and expectations of password expiration schedules to avoid filling up the call center the first Monday morning every 90 days.

Data Handling

User training should address legal or regulatory requirements for accessing, transporting, storing, or disposing of data and data storage devices. This includes encryption systems for mobile and removable storage devices, data access logging requirements under laws such as HIPPA, and review of the retention and destruction policy.

Clean Desk

Training should include details of the organization's clean desk policy, encouraging users to avoid jotting down hard-to-recall passphrases or details from electronic systems that might contain PII. Users should also understand why taping a list of their logons and passwords under their keyboards is a bad idea.

Situational Awareness

User training should encourage situational awareness at all times. Unbadged individuals wandering in secured areas should be challenged, tailgating at check-points (following an authorized individual in closely to avoid having to provide personal authorization credentials) should be prevented, and guidelines for handling other forms of physical and logical security violations must be conveyed and practiced.

Personal Technologies

Common mobile computing devices, removable media storage key fobs; file-sharing systems such as Dropbox, Box.com, or SkyDrive; peer-to-peer transfer services; and even browser-based social media solutions and games can all introduce a range of vulnerabilities and threat agents to an enterprise without

requiring elevated privilege or special equipment. Users must be given training in the proper use of their various personal technologies (or reasons to not use the technologies). Because this area is constantly evolving, convey reminders and updates in the regular security-awareness newsletter.

Users must be trained in critical consideration before providing logon credentials to any service, particularly those that bring personal data interaction into the work-place. Social media services are increasingly used for business purposes, so separation of business and personal accounts become critical in the event of a legal motion for discovery that could otherwise require access to personally controlled data resources. Social media services accessed through encrypted web access also offer a route through which protected information could be inadvertently disclosed without passing in readable form through normal boundary content review systems.

Peer-to-peer (P2P) services also present a danger to intellectual property and system availability protection by allowing direct connections between random endpoints using a wide variety of protocols and service ports, making firewall and packet-shaper management much more difficult for technicians and potentially sharing otherwise secure data stores to unknown parties as in the case of a misconfigured P2P client such as BitTorrent. P2P encrypted data streams can also result in contraband content being placed on a system within an organization without proper review, potentially exposing the organization to legal action based on the type of contraband.

Threat Awareness and Zero-Day Threats

Emergent viruses, worms, Trojans, rootkits, phishing attacks, and other threats should be identified and conveyed to users as rapidly as possible before dozens of calls come in asking why the “I Love You” email didn’t show its attached greeting card properly when opened. Personalized spear-phishing attacks are becoming more prevalent, requiring vigilance on the part of the users to avoid the natural response of opening everything that seems to be coming from their family members, boss, or co-workers. This must be tempered, though, as the million-plus new viral versions every year will rapidly overwhelm users into a state of helplessness or disinterest in the face of apparent inevitability. When a new Zero-Day threat emerges that has not been specifically considered in response planning, the same communication channels can be used to alert users of actions being taken by the IT group to correct, recover, repair, or patch systems and data.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following is *not* going to be part of a standard password policy?
   - ❍ **A.** Establishing a minimum password length
   - ❍ **B.** Selection of a strong password
   - ❍ **C.** Establishing password expiration schedules
   - ❍ **D.** Barring keeping written passwords

2. When conducting data handling training and reviewing disposal practices, what consideration must be primary?
   - ❍ **A.** Breaches of health and safety protocols
   - ❍ **B.** Remnants of data that may remain accessible
   - ❍ **C.** Accidental disposal of equipment that is necessary to read archived legacy data
   - ❍ **D.** Disposal costs and penalties arising from regulatory mandates

3. _____ training teaches users not to download links from social media sites.
   - ❍ **A.** Data handling
   - ❍ **B.** Clean desk
   - ❍ **C.** Situational awareness
   - ❍ **D.** Personal technology

4. When an employee discovers someone wandering around a secured area without a badge or escort, which user-awareness training topic should provide them with knowledge of the proper response?
   - ❍ **A.** Data handling
   - ❍ **B.** Clean desk
   - ❍ **C.** Situational awareness
   - ❍ **D.** Personal technology

Cram Quiz Answers

1. **D**. The clean desk policy includes details regarding written residue of passcodes, PII, and other sensitive data that might be jotted down during normal business. Answers A, B, and C are all incorrect because the question asks which is *not* a part of the password policy, and all three would be found in the password policy: password length, strength criteria, and password duration before expiration.

2. **A**. Because of the materials involved in the manufacturing and construction of electronic equipment, health, and safety protocols take precedence over the other considerations. Health and safety must always come first. Answer B is incorrect because it is concerned with data confidentiality. Answer C is incorrect because it is concerned with data availability, and answer D is incorrect because it focuses on risks and costs arising from regulation.
3. **D**. Personal technology training should cover social networks, peer-to-peer networking, and mobile technologies owned by the employees but present in the workplace. Answer A is incorrect because the data handling training would be focused on how to manage data stored on organizational systems rather than personal ones. Answer B is incorrect because the clean desk policy provides guidance for data sanitization of the work environment. Answer C is incorrect because situational awareness training involves developing strategies and skills for dealing with physical access violations and similar events rather than addressing which personal technologies are appropriate and how they should be used properly.
4. **C**. Situational-awareness training focuses on strategies and skills for dealing with physical access violations, variations from normal operational routines, and similar events. Answer A is incorrect because data handling training is focused on how to manage data stored on organizational systems rather than how to deal with unauthorized personnel in secure areas. Answer B is incorrect because the clean desk policy provides guidance for data sanitization of the work environment to protect against unauthorized data disclosure should an unauthorized individual gain access. Answer D is incorrect because personal technology training provides strategies for dealing with personal technology and services within the organizational enterprise environment.

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the CD. You can also create a custom exam by objective with the practice exam software. Note any objective you struggle with and go to that objective material in this chapter.

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