ROBIN ABERNATHY
TROY McMILLAN

APPROVED
CompTIA
QUALITY CONTENT

Cert Guide

Learn, prepare, and practice for exam success

CompTIA® Advanced Security Practitioner (CASP) CAS-003

CompTIA
CASP

PEARSON IT
CERTIFICATION

FREE SAMPLE CHAPTER

CompTIA® Advanced Security Practitioner (CASP) CAS-003 Cert Guide

Robin Abernathy

Troy McMillan

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA® Advanced Security Practitioner (CASP) CAS-003 Cert Guide

ISBN-13: 978-0-7897-5944-3

ISBN-10: 0-7897-5944-6

Library of Congress Control Number: 2018932405

01 18

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Windows is a registered trademark of Microsoft Corporation.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-In-Chief
Mark Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Michelle Newcomb

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Ken Johnson

Proofreader
Debbie Williams

Technical Editors
Chris Crayton

Publishing Coordinator
Vanessa Evans

Designer
Chuti Prasertsith

Composition
Tricia Bronkella

Contents at a Glance

Online-only Elements:

Table of Contents

Online-only Elements:

About the Authors

Robin Abernathy, CASP, is a product developer and technical editor for Kaplan IT training. She has developed and reviewed certification preparation materials in a variety of product lines, including Microsoft, CompTIA, Cisco, ITIL, (ISC)^2, and PMI, and holds multiple certifications from these vendors. Her work with Kaplan IT Training includes practice tests and study guides for the Transcender brands.

Robin most recently co-authored Pearson's *CISSP Cert Guide* with Troy McMillan and Sari Green and authored Pearson's *Project+ Cert Guide*. She provides training on computer hardware, software, networking, security, and project management. Robin also presents at technical conferences and hosts webinars on IT certification topics. More recently, Robin has recorded videos for CyberVista's IT certification training courses.

Troy McMillan, CASP, is a product developer and technical editor for Kaplan IT Training as well as a full-time trainer. He became a professional trainer more than 15 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. His recent work includes:

- Contributing subject matter expert for *CCNA Cisco Certified Network Associate Certification Exam Preparation Guide* (Kaplan)
- Prep test question writer for *Network+ Study Guide* (Sybex)
- Technical editor for *Windows 7 Study Guide* (Sybex)
- Contributing author for *CCNA-Wireless Study Guide* (Sybex)
- Technical editor for *CCNA Study Guide*, *Revision 7* (Sybex)
- Author of *VCP VMware Certified Professional on vSphere 4 Review Guide: Exam VCP-410* and associated instructional materials (Sybex)
- Author of *Cisco Essentials* (Sybex)
- Co-author of *CISSP Cert Guide* (Pearson)
- Prep test question writer for *CCNA Wireless 640-722* (Cisco Press)

He also has appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND 1; ICND 2; and Cloud+.

He now creates certification practice tests and study guides for the Transcender brands. Troy lives in both Sugarloaf Key, Florida, and Pfafftown, North Carolina, with his wife, Heike.

Dedication

For my husband, Michael, and my son, Jonas. I love you both!
—Robin

I dedicate this book to my wife, who worked tirelessly recovering us from Hurricane Irma. I love you, honey!
—Troy

Acknowledgments

First, I once again thank my heavenly Father for blessing me throughout my life.

I would also like to thank all my family members, many of whom wondered where their acknowledgement was in the *CISSP Cert Guide*. To my siblings, Libby McDaniel Loggins and Kenneth McDaniel: Thanks for putting up with my differences and loving me anyway. To their spouses, Dave Loggins and Michelle Duncan McDaniel, thanks for choosing my siblings and deciding to still stay with them, even when you realized I was part of the package. LOL! To my husband's family, I thank you for accepting me into your family. James and Sandra Abernathy, thanks for raising such a wonderful man. Cathy Abernathy Bonds and Tony Abernathy, thanks for helping to shape him into the man he is. Tony, you are missed more than you will ever know!

I must thank my wonderful husband, Michael, and son, Jonas, for once again being willing to do "guy things" while I was locked away in the world of CASP. You are my world! What a wonderful ride we are on!!!

Thanks to all at Pearson for once again assembling a wonderful team to help Troy and me get through this CASP journey.

To you, the reader, I wish you success in your IT certification goals!

—Robin Abernathy

I must thank my coworkers at Kaplan IT Training, who have helped me to grow over the past 15 years. Thank you, Ann, George, John, Josh, Robin, and Shahara. I also must as always thank my beautiful wife, who has supported me through the lean years and continues to do so. Finally, I have to acknowledge all the help and guidance from the Pearson team.

—Troy McMillan

About the Reviewer

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

We Want to Hear from You!

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

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

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

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

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789759443 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

About the Book

The CompTIA Advanced Security Practitioner (CASP) certification is a popular certification for those in the security field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA CASP certification is unique in that it is vendor neutral. The CompTIA CASP certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by ISC^2.

In the CompTIA CASP exam, the topics are mostly generic in that they can apply to many security devices and technologies, regardless of vendor. Although the CompTIA CASP is vendor neutral, devices and technologies are implemented by multiple independent vendors. In that light, several of the examples associated with this book include using particular vendors' configurations and technologies. More detailed training regarding a specific vendor's software and hardware can be found in books and training specific to that vendor.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the CASP CAS-003 blueprint from CompTIA. This book also helps you demonstrate your knowledge by passing the CAS-003 version of the CompTIA CASP exam.

To aid you in mastering and understanding the CASP + certification objectives, this book provides the following tools:

- **Opening topics list:** This list defines the topics that are covered in the chapter.
- **Key Topics icons:** These icons indicate important figures, tables, and lists of information that you need to know for the exam. They are sprinkled throughout each chapter and are summarized in table format at the end of each chapter.
- **Memory tables:** These can be found on the companion website and in Appendix B, "Memory Tables," and Appendix C, "Memory Tables Answer Key." Use them to help memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the Glossary.

For current information about the CompTIA CASP certification exam, visit https://certification.comptia.org/certifications/comptia-advanced-security-practitioner.

Who Should Read This Book?

Readers of this book will range from people who are attempting to attain a position in the IT security field to people who want to keep their skills sharp or perhaps retain their job when a company policy mandates that they take the new exams.

This book is also for readers who want to acquire additional certifications beyond the CASP certification (for example, the CISSP certification and beyond). The book is designed in such a way to offer easy transition to future certification studies.

Strategies for Exam Preparation

Read the chapters in this book, jotting down notes with key concepts or configurations on a separate notepad.

Download the current list of exam objectives by submitting a form at http://certification.comptia.org/examobjectives.aspx.

Use the practice exam, which is included on this book's companion website. As you work through the practice exam, note the areas where you lack confidence and review those concepts. After you review these areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through a practice exam, the more familiar the questions become, and the practice exam becomes a less accurate indicator of your skills.

After you work through a practice exam a second time and feel confident with your skills, schedule the real CompTIA CASP exam (CAS-003). The following website provides information about registering for the exam: www.pearsonvue.com/comptia/.

CompTIA CASP Exam Topics

Table 1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA CASP CAS-003 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters.

Table 1 CompTIA CASP Exam Topics

Chapter	CAS-003 Exam Objective	CAS-003 Exam Subobjective
1 Business and Industry Influences and Associated Security Risks	1.1 Summarize business and industry influences and associated security risks.	■ Risk management of new products, new technologies and user behaviors ■ New or changing business models/strategies ■ Security concerns of integrating diverse industries ■ Internal and external influences ■ Impact of de-perimeterization (e.g., constantly changing network boundary)
2 Security, Privacy Policies, and Procedures	1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements.	■ Policy and process life cycle management ■ Support legal compliance and advocacy by partnering with human resources, legal, management and other entities ■ Understand common business documents to support security ■ Research security requirements for contracts ■ Understand general privacy principles for sensitive information ■ Support the development of policies containing standard security practices
3 Risk Mitigation Strategies and Controls	1.3 Given a scenario, execute risk mitigation strategies and controls.	■ Categorize data types by impact levels based on CIA ■ Incorporate stakeholder input into CIA impact-level decisions ■ Determine minimum-required security controls based on aggregate score ■ Select and implement controls based on CIA requirements and organizational policies ■ Extreme scenario planning/worst-case scenario ■ Conduct system-specific risk analysis ■ Make risk determination based upon known metrics ■ Translate technical risks in business terms ■ Recommend which strategy should be applied based on risk appetite ■ Risk management processes ■ Continuous improvement/monitoring ■ Business continuity planning ■ IT governance ■ Enterprise resilience

Chapter	CAS-003 Exam Objective	CAS-003 Exam Subobjective
4 Risk Metric Scenarios to Secure the Enterprise	1.4 Analyze risk metric scenarios to secure the enterprise.	■ Review effectiveness of existing security controls ■ Reverse engineer/deconstruct existing solutions ■ Creation, collection and analysis of metrics ■ Prototype and test multiple solutions ■ Create benchmarks and compare to baselines ■ Analyze and interpret trend data to anticipate cyber defense needs ■ Analyze security solution metrics and attributes to ensure they meet business needs ■ Use judgment to solve problems where the most secure solution is not feasible
5 Network and Security Components, Concepts, and Architectures	2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.	■ Physical and virtual network and security devices ■ Application and protocol-aware technologies ■ Advanced network design (wired/wireless) ■ Complex network security solutions for data flow ■ Secure configuration and baselining of networking and security components ■ Software-defined networking ■ Network management and monitoring tools ■ Advanced configuration of routers, switches and other network devices ■ Security zones ■ Network access control ■ Network-enabled devices ■ Critical infrastructure
6 Security Controls for Host Devices	2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements.	■ Trusted OS (e.g., how and when to use it) ■ Endpoint security software ■ Host hardening ■ Boot loader protections ■ Vulnerabilities associated with hardware ■ Terminal services/application delivery services

Chapter	CAS-003 Exam Objective	CAS-003 Exam Subobjective
7 Security Controls for Mobile and Small Form Factor Devices	2.3 Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.	■ Enterprise mobility management ■ Security implications/privacy concerns ■ Wearable technology
8 Software Vulnerability Security Controls	2.4 Given software vulnerability scenarios, select appropriate security controls.	■ Application security design considerations ■ Specific application issues ■ Application sandboxing ■ Secure encrypted enclaves ■ Database activity monitor ■ Web application firewalls ■ Client-side processing vs. server-side processing ■ Operating system vulnerabilities ■ Firmware vulnerabilities
9 Security Assessments	3.1 Given a scenario, conduct a security assessment using the appropriate methods.	■ Methods ■ Types
10 Select the Appropriate Security Assessment Tool	3.2 Analyze a scenario or output, and select the appropriate tool for a security assessment.	■ Network tool types ■ Host tool types ■ Physical security tools
11 Incident Response and Recovery	3.3 Given a scenario, implement incident response and recovery procedures.	■ E-discovery ■ Data breach ■ Facilitate incident detection and response ■ Incident and emergency response ■ Incident response support tools ■ Severity of incident or breach ■ Post-incident response

Chapter	CAS-003 Exam Objective	CAS-003 Exam Subobjective
12 Host, Storage, Network, and Application Integration	4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.	■ Adapt data flow security to meet changing business needs ■ Standards ■ Interoperability issues ■ Resilience issues ■ Data security considerations ■ Resources provisioning and deprovisioning ■ Design considerations during mergers, acquisitions and demergers/divestitures ■ Network secure segmentation and delegation ■ Logical deployment diagram and corresponding physical deployment diagram of all relevant devices ■ Security and privacy considerations of storage integration ■ Security implications of integrating enterprise applications
13 Cloud and Virtualization Technology Integration	4.2 Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.	■ Technical deployment models (outsourcing/insourcing/managed services/partnership) ■ Security advantages and disadvantages of virtualization ■ Cloud augmented security services ■ Vulnerabilities associated with comingling of hosts with different security requirements ■ Data security considerations ■ Resources provisioning and deprovisioning
14 Authentication and Authorization Technology Integration	4.3 Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.	■ Authentication ■ Authorization ■ Attestation ■ Identity proofing ■ Identity propagation ■ Federation ■ Trust models

Chapter	CAS-003 Exam Objective	CAS-003 Exam Subobjective
15 Cryptographic Techniques	4.4 Given a scenario, implement cryptographic techniques.	■ Techniques ■ Implementations
16 Secure Communication and Collaboration	4.5 Given a scenario, select the appropriate control to secure communications and collaboration solutions.	■ Remote access ■ Unified collaboration tools
17 Industry Trends and Their Impact to the Enterprise	5.1 Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.	■ Perform ongoing research ■ Threat intelligence ■ Research security implications of emerging business tools ■ Global IA industry/community
18 Security Activities Across the Technology Life Cycle	5.2 Given a scenario, implement security activities across the technology life cycle.	■ Systems development life cycle ■ Software development life cycle ■ Adapt solutions to address: emerging threats, disruptive technologies, and security trends ■ Asset management (inventory control)
19 Business Unit Interaction	5.3 Explain the importance of interaction across diverse business units to achieve security goals.	■ Interpreting security requirements and goals to communicate with stakeholders from other disciplines ■ Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls ■ Establish effective collaboration within teams to implement secure solutions ■ Governance, risk and compliance committee

How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use.

In addition to the 19 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The companion website also includes a practice test and memory tables that you can work through to verify your knowledge of the subject matter.

Companion Website

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

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: **9780789759443**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

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

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

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software, containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

NOTE The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams 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.

Accessing the Pearson Test Prep Software Online

The online version of the Pearson Test Prep software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to http://www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.
3. Enter the email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you need to establish one by going to PearsonITCertification.com/join.
4. In the **My Products** tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is now listed in your My Products page.
6. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser: http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip.

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: **9780789759443**.

2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. When the software finishes downloading, unzip all the files on your computer.
7. Double-click the application file to start the installation and follow the on-screen instructions to complete the registration.
8. When the installation is complete, launch the application and click **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then the **Finish** button to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

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

- Study Mode
- Practice Exam Mode
- Flash Card Mode

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

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

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

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

Updating Your Exams

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

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Again, this is only an issue with the desktop Windows application.

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

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the chapter questions at the end of each chapter and to review the foundation and key topics. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

This page intentionally left blank

This chapter covers the following topics:

- **The Goals of the CASP Certification**: This section describes CASP's sponsoring bodies and the stated goals of the certification.
- **The Value of the CASP Certification:** This section examines the career and business drivers for the CASP certification.
- **CASP Exam Objectives:** This section lists the official objectives covered on the CASP exam.
- **Steps to Becoming a CASP:** This section explains the process involved in achieving the CASP certification.
- **CompTIA Authorized Materials Use Policy:** This section provides information on the CompTIA Certification Exam Policies web page.

The CASP Exam

The CompTIA Certified Advanced Security Practitioner (CASP) exam is designed to identify IT professionals with advanced-level competency in enterprise security; risk management; incident response; research and analysis; and integration of computing, communications, and business disciplines.

As the number of security threats to organizations grows and the nature of these threats broadens, companies large and small have realized that security can no longer be an afterthought. It must be built into the DNA of the enterprise to be successful. This means trained professionals must not only be versed in security theory but must also be able to implement measures that provide enterprisewide security. While no prerequisites exist to take the exam, it is often the next step for many security professionals after passing the CompTIA Security+ exam.

The Goals of the CASP Certification

The CASP exam is a vendor-neutral exam created and managed by CompTIA. An update to the CASP certification exam launched April 2, 2018. The new exam, CAS-003, replaces CAS-002, which will retire in October 2018. This book is designed to prepare you for the new exam, CAS-003, but can also be used to prepare for the CAS-002 exam. This certification is considered a mastery- or advanced-level certification.

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

Sponsoring Bodies

CompTIA is an American National Standards Institute (ANSI)-accredited certifier that creates and maintains a wide array of IT certification exams, such as A+, Network+, Server+, and Security+. The credentials obtained by passing these various exams are recognized in the industry as demonstrating the skills tested in these exams.

Other Security Exams

The CASP exam is one of several security-related exams that can validate a candidate's skills and knowledge. The following are some of the most popular ones, to put the CASP exam in proper perspective:

- **Certified Information Systems Security Professional (CISSP); ISC^2:** This is a globally recognized standard of achievement that confirms an individual's knowledge in the field of information security. CISSPs are information assurance professionals who define the architecture, design, management, and/or controls that assure the security of business environments. It was the first certification in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024.
- **Security+ (CompTIA):** This exam covers the most important foundational principles for securing a network and managing risk. Access control, identity management, and cryptography are important topics on the exam, along with a selection of appropriate mitigation and deterrent techniques to address network attacks and vulnerabilities.
- **Certified Ethical Hacker (CEH; EC Council):** This exam validates the skills of an ethical hacker. Such individuals are usually trusted people who are employed by organizations to undertake attempts to penetrate networks and/or computer systems using the same methods and techniques as unethical hackers.

Stated Goals

CompTIA's stated goal (verbatim from the CompTIA CASP web page) is as follows:

> Successful candidates will have the knowledge required to:
>
> - Conceptualize, engineer, integrate and implement secure solutions across complex enterprise environments
> - Apply critical thinking and judgment across a broad spectrum of security disciplines to propose and implement sustainable security solutions that map to organizational strategies

- Translate business needs into security requirements
- Analyze risk impact
- Respond to security incidents

The Value of the CASP Certification

The CASP certification holds value for both the exam candidate and the enterprise. The CASP certification has been approved by the U.S. Department of Defense to meet Information Assurance (IA) technical and management certification requirements and has been chosen by Dell and HP advanced security personnel. Advantages can be gained by both the candidate and the organization employing the candidate.

To the Security Professional

There are numerous reasons a security professional would spend the time and effort required to achieve this credential. Here are some of them:

- To meet the growing demand for security professionals
- To become more marketable in an increasingly competitive job market
- To enhance skills in a current job
- To qualify for or compete more successfully for a promotion
- To increase salary

Department of Defense Directive 8140 and 8570 (DoDD 8140 and 8570)

DoDD 8140 and 8750 workforce qualification requirements both prescribe that members of the military who hold certain job roles must hold security certifications. The directive lists the CASP certification at several levels. Figure I-1 shows job roles that require various certifications, including CASP.

IAT Level I	IAT Level II	IAT Level III
• *CompTIA* **A+** • *CompTIA* **Network+** • Cisco Certified Network Associate–Security (**CCNA Security**) • (*ISC*)*2* Systems Security Certified Practitioner (**SSCP**)	• *Cisco* Certified Network Associate–Security (**CCNA Security**) • GIAC Global Security Cyber Security Professional (**GICSP**) • GIAC Security Essentials (**GSEC**) • *CompTIA* **Security+** • (*ISC*)*2* Systems Security Certified Practitioner (**SSCP**)	• CompTIA Advanced Security Practitioner (**CASP**) • *ISACA* Certified Information Systems Auditor (**CISA**) • (*ISC*)*2* Certified Information Systems Security Professional (**CISSP**) (or Associate) • *GIAC* Certified Enterprise Defender (**GCED**) • *GIAC* Certified Incident Handler (**GCIH**)

IAM Level I	IAM Level II	IAM Level III
• (*ISC*)*2* Certified Authorization Professional (**CAP**) • *GIAC* Security Leadership (**GSLC**) • Comp*TIA* **Security+**	• (*ISC*)*2* Certified Authorization Professional (**CAP**) • CompTIA Advanced Security Practitioner (**CASP**) • *ISACA* Certified Information Security Manager (**CISM**) • (*ISC*)*2* Certified Information Systems Security Professional (**CISSP**) (or Associate) • *GIAC* Security Leadership (**GSLC**)	• *ISACA* Certified Information Security Manager (**CISM**) • (*ISC*)*2* Certified Information Systems Security Professional (**CISSP**) (or Associate) • *GIAC* Security Leadership (**GSLC**)

IASAE I	IASAE II	IASAE III
• CompTIA Advanced Security Practitioner (**CASP**) • (*ISC*)*2* Certified Information Systems Security Professional (**CISSP**) (or Associate) • (*ISC*)*2* Certified Secure Software Lifecycle Professional (**CSSLP**)	• CompTIA Advanced Security Practitioner (**CASP**) • (*ISC*)*2* Certified Information Systems Security Professional (**CISSP**) (or Associate) • (*ISC*)*2* Certified Secure Software Lifecycle Professional (**CSSLP**)	• (*ISC*)*2* Certified Information Systems Security Professional–Architecture (**CISSP-ISSAP**) • (*ISC*)*2* Certified Information Systems Security Professional–Engineering (**CISSP-ISSEP**)

Figure I-1 DoDD 8570

In short, the CASP certification demonstrates that the holder has the knowledge and skills tested in the exam and also that the candidate has hands-on experience and can organize and implement a successful security solution.

To the Enterprise

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

CASP Exam Objectives

The material contained in the CASP exam objectives is divided into five domains. The following pages outline the objectives tested in each of the domains for the CAS-003 exam.

1.0 Risk Management

1.1 Summarize business and industry influences and associated security risks.

- Risk management of new products, new technologies and user behaviors
- New or changing business models/strategies
  - Partnerships
  - Outsourcing
  - Cloud
  - Acquisition/merger–divestiture/demerger
    - Data ownership
    - Data reclassification
- Security concerns of integrating diverse industries
  - Rules
  - Policies
  - Regulations
    - Export controls
    - Legal requirements
  - Geography
    - Data sovereignty
    - Jurisdictions
- Internal and external influences
  - Competitors
  - Auditors/audit findings
  - Regulatory entities
  - Internal and external client requirements
  - Top-level management

- Impact of de-perimeterization (e.g., constantly changing network boundary)
  - Telecommuting
  - Cloud
  - Mobile
  - BYOD
  - Outsourcing
  - Ensuring third-party providers have requisite levels of information security

1.2 Compare and contrast security, privacy policies and procedures based on organizational requirements.

- Policy and process life cycle management
  - New business
  - New technologies
  - Environmental changes
  - Regulatory requirements
  - Emerging risks
- Support legal compliance and advocacy by partnering with human resources, legal, management and other entities
- Understand common business documents to support security
  - Risk assessment (RA)
  - Business impact analysis (BIA)
  - Interoperability agreement (IA)
  - Interconnection security agreement (ISA)
  - Memorandum of understanding (MOU)
  - Service-level agreement (SLA)
  - Operating-level agreement (OLA)
  - Non-disclosure agreement (NDA)
  - Business partnership agreement (BPA)
  - Master service agreement (MSA)

- Research security requirements for contracts
  - Request for proposal (RFP)
  - Request for quote (RFQ)
  - Request for information (RFI)
- Understand general privacy principles for sensitive information
- Support the development of policies containing standard security practices
  - Separation of duties
  - Job rotation
  - Mandatory vacation
  - Least privilege
  - Incident response
  - Forensic tasks
  - Employment and termination procedures
  - Continuous monitoring
  - Training and awareness for users
  - Auditing requirements and frequency
  - Information classification

1.3 Given a scenario, execute risk mitigation strategies and controls.

- Categorize data types by impact levels based on CIA
- Incorporate stakeholder input into CIA impact-level decisions
- Determine minimum-required security controls based on aggregate score
- Select and implement controls based on CIA requirements and organizational policies
- Extreme scenario planning/worst-case scenario
- Conduct system-specific risk analysis
- Make risk determination based upon known metrics
  - Magnitude of impact based on ALE and SLE
  - Likelihood of threat

    - Motivation
    - Source
    - ARO
    - Trend analysis
  - Return on investment (ROI)
  - Total cost of ownership
- Translate technical risks in business terms
- Recommend which strategy should be applied based on risk appetite
  - Avoid
  - Transfer
  - Mitigate
  - Accept
- Risk management processes
  - Exemptions
  - Deterrence
  - Inherent
  - Residual
- Continuous improvement/monitoring
- Business continuity planning
  - RTO
  - RPO
  - MTTR
  - MTBF
- IT governance
  - Adherence to risk management frameworks
- Enterprise resilience

1.4 Analyze risk metric scenarios to secure the enterprise.

- Review effectiveness of existing security controls
  - Gap analysis
  - Lessons learned
  - After-action reports
- Reverse engineer/deconstruct existing solutions
- Creation, collection and analysis of metrics
  - KPIs
  - KRIs
- Prototype and test multiple solutions
- Create benchmarks and compare to baselines
- Analyze and interpret trend data to anticipate cyber defense needs
- Analyze security solution metrics and attributes to ensure they meet business needs
  - Performance
  - Latency
  - Scalability
  - Capability
  - Usability
  - Maintainability
  - Availability
  - Recoverability
  - ROI
  - TCO
- Use judgment to solve problems where the most secure solution is not feasible

2.0 Enterprise Security Architecture

2.1 Analyze a scenario and integrate network and security components, concepts and architectures to meet security requirements.

- Physical and virtual network and security devices
  - UTM
  - IDS/IPS
  - NIDS/NIPS
  - INE
  - NAC
  - SIEM
  - Switch
  - Firewall
  - Wireless controller
  - Router
  - Proxy
  - Load balancer
  - HSM
  - MicroSD HSM
- Application and protocol-aware technologies
  - WAF
  - Firewall
  - Passive vulnerability scanners
  - DAM
- Advanced network design (wired/wireless)
  - Remote access
    - VPN
      - IPSec
      - SSL/TLS

    - SSH
    - RDP
    - VNC
    - VDI
    - Reverse proxy
  - IPv4 and IPv6 transitional technologies
  - Network authentication methods
  - 802.1x
  - Mesh networks
  - Placement of fixed/mobile devices
  - Placement of hardware and applications
- Complex network security solutions for data flow
  - DLP
  - Deep packet inspection
  - Data flow enforcement
  - Network flow (S/flow)
  - Data flow diagram
- Secure configuration and baselining of networking and security components
- Software-defined networking
- Network management and monitoring tools
  - Alert definitions and rule writing
  - Tuning alert thresholds
  - Alert fatigue
- Advanced configuration of routers, switches and other network devices
  - Transport security
  - Trunking security
  - Port security
  - Route protection

    - DDoS protection
    - Remotely triggered black hole
- Security zones
    - DMZ
    - Separation of critical assets
    - Network segmentation
- Network access control
    - Quarantine/remediation
    - Persistent/volatile or non-persistent agent
    - Agent vs. agentless
- Network-enabled devices
    - System on a chip (SoC)
    - Building/home automation systems
    - IP video
    - HVAC controllers
    - Sensors
    - Physical access control systems
    - A/V systems
    - Scientific/industrial equipment
- Critical infrastructure
    - Supervisory control and data acquisition (SCADA)
    - Industrial control systems (ICS)

2.2 Analyze a scenario to integrate security controls for host devices to meet security requirements.

- Trusted OS (e.g., how and when to use it)
    - SELinux
    - SEAndroid
    - TrustedSolaris
    - Least functionality

- Endpoint security software
  - Anti-malware
  - Antivirus
  - Anti-spyware
  - Spam filters
  - Patch management
  - HIPS/HIDS
  - Data loss prevention
  - Host-based firewalls
  - Log monitoring
  - Endpoint detection response
- Host hardening
  - Standard operating environment/configuration baselining
    - Application whitelisting and blacklisting
  - Security/group policy implementation
  - Command shell restrictions
  - Patch management
    - Manual
    - Automated
      - Scripting and replication
  - Configuring dedicated interfaces
    - Out-of-band management
    - ACLs
    - Management interface
    - Data interface

    - External I/O restrictions
        - USB
        - Wireless
            - Bluetooth
            - NFC
            - IrDA
            - RF
            - 802.11
            - RFID
        - Drive mounting
        - Drive mapping
        - Webcam
        - Recording mic
        - Audio output
        - SD port
        - HDMI port
    - File and disk encryption
    - Firmware updates
- Boot loader protections
    - Secure boot
    - Measured launch
    - Integrity measurement architecture
    - BIOS/UEFI
    - Attestation services
    - TPM
- Vulnerabilities associated with hardware
- Terminal services/application delivery services

2.3 Analyze a scenario to integrate security controls for mobile and small form factor devices to meet security requirements.

- Enterprise mobility management
  - Containerization
  - Configuration profiles and payloads
  - Personally owned, corporate-enabled
  - Application wrapping
  - Remote assistance access
    - VNC
    - Screen mirroring
  - Application, content and data management
  - Over-the-air updates (software/firmware)
  - Remote wiping
  - SCEP
  - BYOD
  - COPE
  - VPN
  - Application permissions
  - Side loading
  - Unsigned apps/system apps
  - Context-aware management
    - Geolocation/geofencing
    - User behavior
    - Security restrictions
    - Time-based restrictions
- Security implications/privacy concerns
  - Data storage
    - Non-removable storage
    - Removable storage

  - Cloud storage
  - Transfer/backup data to uncontrolled storage
  - USB OTG
- Device loss/theft
- Hardware anti-tamper
  - eFuse
- TPM
- Rooting/jailbreaking
- Push notification services
- Geotagging
- Encrypted instant messaging apps
- Tokenization
- OEM/carrier Android fragmentation
- Mobile payment
  - NFC-enabled
  - Inductance-enabled
  - Mobile wallet
  - Peripheral-enabled payments (credit card reader)
- Tethering
  - USB
  - Spectrum management
  - Bluetooth 3.0 vs. 4.1
- Authentication
  - Swipe pattern
  - Gesture
  - Pin code
  - Biometric
    - Facial
    - Fingerprint
    - Iris scan

        - Malware
        - Unauthorized domain bridging
        - Baseband radio/SOC
        - Augmented reality
        - SMS/MMS/messaging
- Wearable technology
    - Devices
        - Cameras
        - Watches
        - Fitness devices
        - Glasses
        - Medical sensors/devices
        - Headsets
    - Security implications
        - Unauthorized remote activation/deactivation of devices or features
        - Encrypted and unencrypted communication concerns
        - Physical reconnaissance
        - Personal data theft
        - Health privacy
        - Digital forensics of collected data

2.4 Given software vulnerability scenarios, select appropriate security controls.

- Application security design considerations
    - Secure: by design, by default, by deployment
- Specific application issues
    - Unsecure direct object references
    - XSS
    - Cross-site request forgery (CSRF)
    - Click-jacking

    - Session management
    - Input validation
    - SQL injection
    - Improper error and exception handling
    - Privilege escalation
    - Improper storage of sensitive data
    - Fuzzing/fault injection
    - Secure cookie storage and transmission
    - Buffer overflow
    - Memory leaks
    - Integer overflows
    - Race conditions
        - Time of check
        - Time of use
    - Resource exhaustion
    - Geotagging
    - Data remnants
    - Use of third-party libraries
    - Code reuse
- Application sandboxing
- Secure encrypted enclaves
- Database activity monitor
- Web application firewalls
- Client-side processing vs. server-side processing
    - JSON/REST
    - Browser extensions
        - ActiveX
        - Java applets

    - HTML5
    - AJAX
    - SOAP
    - State management
    - JavaScript
- Operating system vulnerabilities
- Firmware vulnerabilities

3.0 Enterprise Security Operations

3.1 Given a scenario, conduct a security assessment using the appropriate methods.

- Methods
    - Malware sandboxing
    - Memory dumping, runtime debugging
    - Reconnaissance
    - Fingerprinting
    - Code review
    - Social engineering
    - Pivoting
    - Open source intelligence
        - Social media
        - Whois
        - Routing tables
        - DNS records
        - Search engines

- Types
  - Penetration testing
    - Black box
    - White box
    - Gray box
  - Vulnerability assessment
  - Self-assessment
    - Tabletop exercises
  - Internal and external audits
  - Color team exercises
    - Red team
    - Blue team
    - White team

3.2 Analyze a scenario or output, and select the appropriate tool for a security assessment.

- Network tool types
  - Port scanners
  - Vulnerability scanners
  - Protocol analyzer
    - Wired
    - Wireless
  - SCAP scanner
  - Network enumerator
  - Fuzzer
  - HTTP interceptor
  - Exploitation tools/frameworks
  - Visualization tools
  - Log reduction and analysis tools

- Host tool types
  - Password cracker
  - Vulnerability scanner
  - Command line tools
  - Local exploitation tools/frameworks
  - SCAP tool
  - File integrity monitoring
  - Log analysis tools
  - Antivirus
  - Reverse engineering tools
- Physical security tools
  - Lock picks
  - RFID tools
  - IR camera

3.3 Given a scenario, implement incident response and recovery procedures.

- E-discovery
  - Electronic inventory and asset control
  - Data retention policies
  - Data recovery and storage
  - Data ownership
  - Data handling
  - Legal holds
- Data breach
  - Detection and collection
    - Data analytics
  - Mitigation
    - Minimize
    - Isolate

  - Recovery/reconstitution
  - Response
  - Disclosure
- Facilitate incident detection and response
  - Hunt teaming
  - Heuristics/behavioral analytics
  - Establish and review system, audit and security logs
- Incident and emergency response
  - Chain of custody
  - Forensic analysis of compromised system
  - Continuity of operations
  - Disaster recovery
  - Incident response team
  - Order of volatility
- Incident response support tools
  - dd
  - tcpdump
  - nbtstat
  - netstat
  - nc (Netcat)
  - memcopy
  - tshark
  - foremost
- Severity of incident or breach
  - Scope
  - Impact
  - Cost
  - Downtime
  - Legal ramifications

- Post-incident response
  - Root-cause analysis
  - Lessons learned
  - After-action report

4.0 Technical Integration of Enterprise Security

4.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture.

- Adapt data flow security to meet changing business needs
- Standards
  - Open standards
  - Adherence to standards
  - Competing standards
  - Lack of standards
  - De facto standards
- Interoperability issues
  - Legacy systems and software/current systems
  - Application requirements
  - Software types
    - In-house developed
    - Commercial
    - Tailored commercial
    - Open source
  - Standard data formats
  - Protocols and APIs
- Resilience issues
  - Use of heterogeneous components
  - Course of action automation/orchestration
  - Distribution of critical assets

    - Persistence and non-persistence of data
    - Redundancy/high availability
    - Assumed likelihood of attack
- Data security considerations
    - Data remnants
    - Data aggregation
    - Data isolation
    - Data ownership
    - Data sovereignty
    - Data volume
- Resources provisioning and deprovisioning
    - Users
    - Servers
    - Virtual devices
    - Applications
    - Data remnants
- Design considerations during mergers, acquisitions and demergers/divestitures
- Network secure segmentation and delegation
- Logical deployment diagram and corresponding physical deployment diagram of all relevant devices
- Security and privacy considerations of storage integration
- Security implications of integrating enterprise applications
    - CRM
    - ERP
    - CMDB
    - CMS
    - Integration enablers
        - Directory services
        - DNS

        - SOA
        - ESB

4.2 Given a scenario, integrate cloud and virtualization technologies into a secure enterprise architecture.

- Technical deployment models (outsourcing/insourcing/managed services/partnership)
    - Cloud and virtualization considerations and hosting options
        - Public
        - Private
        - Hybrid
        - Community
        - Multitenancy
        - Single tenancy
    - On-premise vs. hosted
    - Cloud service models
        - SaaS
        - IaaS
        - PaaS
- Security advantages and disadvantages of virtualization
    - Type 1 vs. Type 2 hypervisors
    - Container-based
    - vTPM
    - Hyperconverged infrastructure
    - Virtual desktop infrastructure
    - Secure enclaves and volumes
- Cloud augmented security services
    - Anti-malware
    - Vulnerability scanning
    - Sandboxing

  - Content filtering
  - Cloud security broker
  - Security as a service
  - Managed security service providers
- Vulnerabilities associated with comingling of hosts with different security requirements
  - VMEscape
  - Privilege elevation
  - Live VM migration
  - Data remnants
- Data security considerations
  - Vulnerabilities associated with a single server hosting multiple data types
  - Vulnerabilities associated with a single platform hosting multiple data types/owners on multiple virtual machines
- Resources provisioning and deprovisioning
  - Virtual devices
  - Data remnants

4.3 Given a scenario, integrate and troubleshoot advanced authentication and authorization technologies to support enterprise security objectives.

- Authentication
  - Certificate-based authentication
  - Single sign-on
  - 802.1x
  - Context-aware authentication
  - Push-based authentication
- Authorization
  - OAuth
  - XACML
  - SPML

- Attestation
- Identity proofing
- Identity propagation
- Federation
  - SAML
  - OpenID
  - Shibboleth
  - WAYF
- Trust models
  - RADIUS configurations
  - LDAP
  - AD

4.4 Given a scenario, implement cryptographic techniques.

- Techniques
  - Key stretching
  - Hashing
  - Digital signature
  - Message authentication
  - Code signing
  - Pseudo-random number generation
  - Perfect forward secrecy
  - Data-in-transit encryption
  - Data-in-memory/processing
  - Data-at-rest encryption
    - Disk
    - Block
    - File
    - Record
  - Steganography

- Implementations
    - Crypto modules
    - Crypto processors
    - Cryptographic service providers
    - DRM
    - Watermarking
    - GPG
    - SSL/TLS
    - SSH
    - S/MIME
    - Cryptographic applications and proper/improper implementations
        - Strength
        - Performance
        - Feasibility to implement
        - Interoperability
    - Stream vs. block
    - PKI
        - Wild card
        - OCSP vs. CRL
        - Issuance to entities
        - Key escrow
        - Certificate
        - Tokens
        - Stapling
        - Pinning
    - Cryptocurrency/blockchain
    - Mobile device encryption considerations
    - Elliptic curve cryptography
        - P256 vs. P384 vs. P512

4.5 Given a scenario, select the appropriate control to secure communications and collaboration solutions.

- Remote access
  - Resource and services
  - Desktop and application sharing
  - Remote assistance
- Unified collaboration tools
  - Conferencing
    - Web
    - Video
    - Audio
  - Storage and document collaboration tools
  - Unified communication
  - Instant messaging
  - Presence
  - Email
  - Telephony and VoIP integration
  - Collaboration sites
    - Social media
    - Cloud-based

5.0 Research, Development and Collaboration

5.1 Given a scenario, apply research methods to determine industry trends and their impact to the enterprise.

- Perform ongoing research
  - Best practices
  - New technologies, security systems and services
  - Technology evolution (e.g., RFCs, ISO)

- Threat intelligence
    - Latest attacks
    - Knowledge of current vulnerabilities and threats
    - Zero-day mitigation controls and remediation
    - Threat model
- Research security implications of emerging business tools
    - Evolving social media platforms
    - Integration within the business
    - Big Data
    - AI/machine learning
- Global IA industry/community
    - Computer emergency response team (CERT)
    - Conventions/conferences
    - Research consultants/vendors
    - Threat actor activities
    - Emerging threat sources

5.2 Given a scenario, implement security activities across the technology life cycle.

- Systems development life cycle
    - Requirements
    - Acquisition
    - Test and evaluation
    - Commissioning/decommissioning
    - Operational activities
        - Monitoring
        - Maintenance
        - Configuration and change management
    - Asset disposal
    - Asset/object reuse

- Software development life cycle
    - Application security frameworks
    - Software assurance
        - Standard libraries
        - Industry-accepted approaches
        - Web services security (WS-security)
        - Forbidden coding techniques
        - NX/XN bit use
        - ASLR use
        - Code quality
        - Code analyzers
            - Fuzzer
            - Static
            - Dynamic
    - Development approaches
        - DevOps
        - Security implications of agile, waterfall and spiral software development methodologies
        - Continuous integration
        - Versioning
    - Secure coding standards
    - Documentation
        - Security requirements traceability matrix (SRTM)
        - Requirements definition
        - System design document
        - Testing plans
    - Validation and acceptance testing
        - Regression
        - User acceptance testing

        - Unit testing
        - Integration testing
        - Peer review
- Adapt solutions to address:
    - Emerging threats
    - Disruptive technologies
    - Security trends
- Asset management (inventory control)

5.3 Explain the importance of interaction across diverse business units to achieve security goals.

- Interpreting security requirements and goals to communicate with stakeholders from other disciplines
    - Sales staff
    - Programmer
    - Database administrator
    - Network administrator
    - Management/executive management
    - Financial
    - Human resources
    - Emergency response team
    - Facilities manager
    - Physical security manager
    - Legal counsel
- Provide objective guidance and impartial recommendations to staff and senior management on security processes and controls
- Establish effective collaboration within teams to implement secure solutions
- Governance, risk and compliance committee

Steps to Becoming a CASP

To become a CASP, there are certain prerequisite procedures to follow. The following sections cover those topics.

Qualifying for the Exam

While there is no required prerequisite, the CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus at the enterprise level.

Signing Up for the Exam

A CompTIA Advanced Security Practitioner (CASP) voucher costs $390.

About the Exam

The following are the characteristics of the exam:

- **Launches:** April 2, 2018
- **Number of questions:** 90 (maximum)
- **Type of questions:** Multiple choice and performance based
- **Length of test:** 165 minutes
- **Passing score:** Pass/fail only; no scaled score
- **Recommended experience:** 10 years' experience in IT administration, including at least 5 years of hands-on technical security experience
- **Languages:** English

CompTIA Authorized Materials Use Policy

CompTIA has recently started a more proactive movement toward preventing test candidates from using brain dumps in their pursuit of certifications. CompTIA currently implements the CompTIA Authorized Quality Curriculum (CAQC) program, whereby content providers like Pearson can submit their test preparation materials to an authorized third party for audit. The CAQC checks to ensure that adequate topic coverage is provided by the content. Only authorized partners can submit their material to the third party.

In the current CAS-003 Blueprint, CompTIA includes a section titled "CompTIA Authorized Materials Use Policy" that says:

> CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

Remember: Just because you purchase a product does not mean that the product is legitimate. Some of the best brain dump companies out there charge for their products. Also, keep in mind that using materials from a brain dump can result in certification revocation. Please make sure that all products you use are from a legitimate provider rather than a brain dump company. Using a brain dump is cheating and directly violates the non-disclosure agreement (NDA) you sign at exam time.

This page intentionally left blank

This chapter covers the following topics:

- **Policy and Process Life Cycle Management:** This section discusses the effects that new business, new technologies, environmental changes, and regulatory requirements have on policy and process life cycle management.
- **Support Legal Compliance and Advocacy:** This section covers partnering with human resources, legal, management, and other entities to support legal compliance.
- **Common Business Documents to Support Security:** The documents discussed in this section include risk assessments/statements of applicability, business impact analyses, interoperability agreements, interconnection security agreements, memorandums of understanding, service-level agreements, operating-level agreements, non-disclosure agreements, business partnership agreements, and master service agreements.
- **Security Requirements for Contracts:** Topics include requests for proposal, requests for quote, requests for information, and agreements.
- **General Privacy Principles for Sensitive Information:** This section explains personally identifiable information and details the privacy principles that are important for protecting PII.
- **Policies Containing Standard Security Practices:** The components discussed include separation of duties, job rotation, mandatory vacation, the principle of least privilege, incident response, forensic tasks, employment and termination procedures, continuous monitoring, training and awareness for users, auditing requirements and frequency, and information classification.

This chapter covers CAS-003 objective 1.2.

CHAPTER 2

Security, Privacy Policies, and Procedures

IT governance documents should be implemented to ensure that organizational assets are protected as well as possible. This chapter explains how the process and policy life cycles are managed and how to support legal compliance. It also discusses business documents and contracts that are commonly used to support security. It covers general privacy principles. Finally, it discusses the development of policies containing standard security practices.

Policy and Process Life Cycle Management

In a top-down approach, management initiates, supports, and directs the security program. In a bottom-up approach, staff members develop a security program prior to receiving direction and support from management. A top-down approach is much more efficient than a bottom-up approach because management's support is one of the most important components of a security program. Using the top-down approach can help ensure that an organization's policies align with its strategic goals.

In the context of organizational security, a *policy* is a course or principle of action adopted by an organization, and a *process* is a series of actions taken to achieve a particular end. A *procedure* is a series of actions conducted in a certain order or manner. Policies, procedures, and processes determine all major decisions and actions within an organization, and all organizational tasks operate within the boundaries set by policies, procedures, and processes.

To understand the relationship between the three, policies are written first to guide the creation of procedures and processes. Processes then provide a high-level view of tasks within the processes. Procedures are the detailed steps involved to complete the process.

Let's look at an example. Say that an organization adopts a particular policy for processing accounts payable. The process designed around this policy details the high-level tasks that must occur, which may include receiving the bill, inputting the bill, authorizing the payment, printing the check, signing the check, and mailing the check. The procedures written would include each separate step involved in each task in the process.

Policies should be written based on the following life cycle:

Step 1. Develop the policy.

Step 2. Perform quality control.

Step 3. Obtain approval of the policy.

Step 4. Publish the policy.

Step 5. Periodically review the policy.

Step 6. Archive the policy when no longer needed or applicable.

During this life cycle, the quality control should be performed prior to obtaining approval to ensure that the policy complies with laws, regulations, and standards. When the policy is published, the organization must ensure that the affected personnel are properly educated on the new policy. The new policy should be incorporated into any training received by these personnel. Each policy should at minimum be reviewed annually. If policies must be changed, version control should be implemented to ensure that the most current version of a policy is being used across the enterprise. When a policy is outdated, it should be archived.

Policies should be reviewed often and on a regular schedule. Certain business, technology, risk, and environment changes should always trigger a review of policies, including adoption of a new technology, merger with another organization, and identification of a new attack method.

For example, suppose that employees request remote access to corporate email and shared drives. If remote access has never been offered but the need to improve productivity and rapidly respond to customer demands means staff now require remote access, the organization should analyze the need to determine whether it is valid. Then, if the organization decides to allow remote access, the organization's security professionals should plan and develop security policies based on the assumption that external environments have active hostile threats.

Policies that should be considered include password policies, data classification policies, wireless and VPN policies, remote access policies, and device access policies. Most organizations develop password and data classification policies first.

A process is a collection of related activities that produce a specific service or product (that is, serve a particular goal) for the organization. Change management and risk management are examples of processes.

Once a policy is written, the appropriate processes should be written based on the following life cycle:

Step 1. Analyze

Step 2. Design

Step 3. Implement

Step 4. Monitor

Step 5. Retire

During this life cycle, step 1 is the time to analyze the policy, and step 2 is the time to design the process based on the policy. When the new process is implemented, all personnel involved in the process should be informed of how the process works. The process should be monitored regularly and may be modified as issues arise or as the base policy has been updated. Keep in mind that processes are created based on the policy. If a new policy is adopted, then a new process is needed. If a policy is edited or archived, then the process for the policy should also be edited or retired.

Once the policy and associated processes are documented, procedures must be written. Procedures embody all the detailed actions that personnel are required to follow and are the closest to the computers and other devices. Procedures often include step-by-step lists on how policies and processes are implemented.

Once an organization has analyzed the business, technology, risk, and environment changes to develop and update policies, the organization must take the next step: Develop and update its processes and procedures in light of the new or updated policies and environment and business changes. Procedures might have to be changed, for example, if the organization upgrades to the latest version of the backup software it uses. Most software upgrades involve analyzing the current procedures and determining how they should be changed. As another example, say that management decides to use more outside contractors to complete work. The organization may need to add a new process within the organization for reviewing the quality of the outside contractor's work. As a final example, suppose that an organization decides to purchase several Linux servers to replace the current Microsoft file servers. While the high-level policies will remain the same, the procedures for meeting those high-level policies will have to be changed.

If an organization's marketing department needs to provide more real-time interaction with its partners and consumers and decides to move forward with a presence on multiple social networking sites for sharing information, the organization would need to establish a specific set of trained people who can release information on the organization's behalf and provide other personnel with procedures and processes for sharing the information.

Some of the processes and procedures that should be considered include the change management process, the configuration management process, network access procedures, wireless access procedures, and database administration procedures. But remember that procedures and processes should be created or changed only after the appropriate policies are adopted. The policies will guide the development of the processes and procedures.

Internal organizational drivers are the basis on which policies and processes are developed. Organizations should ensure that policies and processes are designed or reviewed when new business or business changes occur, new technologies are launched, environmental changes occur, or regulatory requirements change.

New Business

New business occurs when an organization launches or purchases a new area of business. Business changes are changes dictated by the nature of an organization's business and are often driven by consumer demands. As a change occurs, an organization must ensure that it understands the change and its implication for the security posture of the organization. Organizations should take a proactive stance when it comes to these changes. Don't wait for problems. Anticipate the changes and deploy mitigation techniques to help prevent them!

Suppose a business decides to launch a new endeavor whereby consumers can now directly purchase the products that were previously only sold to large retail stores. A new business policy will need to be written based on this new model, and a new process will need to be designed to handle the new business.

Security professionals are integral to any projects wherein new business is starting or business changes are occurring because the security professionals ensure that security controls are considered. Security professionals should ensure that all risks associated with the new business or business change are documented, analyzed, and reported to management. They must also document any suggested security controls that will mitigate these risks.

New Technologies

Technology changes are driven by new technological developments that force organizations to adopt new technologies. Again, organizations must ensure that they understand the changes and their implications for the security posture of the organization.

Suppose a business decides to allow personnel to implement a bring your own device (BYOD) policy. Security professionals should work to ensure that the policy defines the parameters wherein BYOD will be allowed or denied. In addition, the process would need to be written and would likely include obtaining formal approval of a device, assessing the security posture of the device, and granting the device full or limited access based on the device's security posture.

Security professionals are integral to the inclusion or usage of any new technologies because they ensure that security controls will be considered. Security professionals should ensure that all risks associated with new technology are documented, analyzed, and reported to management. They must also suggest and document security controls to mitigate these risks.

Environmental Changes

Environmental changes are divided into two categories: those motivated by the culture in an organization and those motivated by the environment of the industry. As with new business or technologies, organizations must ensure that they understand the changes and their implications for the security posture of the organization.

Suppose a business decides to implement a new policy that provides a certain amount of "green space" for each of its facilities. Management would need to develop a process whereby these green spaces could be completed and maintained. It would likely include purchasing the land, designing the plan for the land, implementing the new green space, and maintaining the green space.

Regulatory Requirements

Regulatory requirements are any requirements that must be documented and followed based on laws and regulations. Standards can also be used as part of the regulatory environment but are not strictly enforced as laws and regulations. As with new business or technologies or environmental changes, organizations must ensure that they understand the regulations and their implications to the security posture of the organization.

The International Organization for Standardization (ISO) has developed a series of standards that are meant to aid organizations in the development of security policies. Other regulatory bodies include local, state, federal, and other government bodies.

Let's look at an example. Suppose an organization is rewriting its security policies and has halted the rewriting progress because the executives believe that the organization's major vendors have a good handle on compliance and regulatory standards. The executive-level managers are allowing vendors to play a large role in writing the organization's policy. However, the IT director decides that while vendor support is important, it is critical that the company write the policy objectively because vendors may not always put the organization's interests first. The IT director should make the following recommendations to senior staff:

- Consult legal and regulatory requirements.
- Draft a general organizational policy.

- Specify functional implementation policies.
- Establish necessary standards, procedures, baselines, and guidelines.

As you can see from this example, you don't have to memorize the specific standards. However, you need to understand how organizations apply them, how they are revised, and how they can be customized to fit organizational needs.

Emerging Risks

Emerging risks are any risks that have emerged due to the recent security landscape. Often risks are not identified for new technologies, devices, and applications until after one of them has been deployed. Organizations should write policies and procedures to ensure that security professionals are doing the proper research to understand emerging risks. Emerging risks is an area that can be particularly dependent upon patch management. Often vendors will try to quickly release security fixes for any emerging risks.

Suppose an organization decides to deploy a new Internet of Things (IoT) device. Several weeks into the deployment, the vendor announces a security flaw that allows attackers to take over the device functionality. As a result, they release a security patch that addresses this issue. If the appropriate policies are in place, the organization's security professionals should be monitoring the vendor for announcements regarding patch management and should deploy the patch once it can be properly tested.

Support Legal Compliance and Advocacy

An organization should involve its human resources department, legal department or legal counsel, senior management, and other internal and external entities in its legal compliance and advocacy program. Legal compliance ensures that an organization follows relevant laws, regulations, and business rules. Legal advocacy is the process carried out by or for an organization that aims to influence public policy and resource allocation decisions in political, economic, and social systems and institutions.

Human resources involvement ensures that the organization is addressing all employment laws and regulations to protect its employees. Human resources professionals can help guide an organization's security policies to ensure that individual rights are upheld while at the same time protecting organizational assets and liability. For example, an organization should ensure that a screen is displayed at login that informs users of the employer's rights to monitor, seize, and search organizational devices to reduce the likelihood of related legal issues. Then, if a technician must take an employee's workstation into custody in response to an investigation, the organization is protected. Both the HR and legal departments should be involved in creating the statement that will be displayed to ensure that it includes all appropriate information.

NOTE Applicable laws are covered in Chapter 1, "Business and Industry Influences and Associated Security Risks." To learn about specific laws that could affect an organization, refer to the section "Legal Requirements."

Common Business Documents to Support Security

Security professionals need to use many common business documents to support the implementation and management of organizational security. Understanding these business documents helps ensure that all areas of security risk are addressed and the appropriate policies, procedures, and processes are developed.

Risk Assessment (RA)

Key Topic

A risk assessment (RA) is a tool used in risk management to identify vulnerabilities and threats, assess the impacts of those vulnerabilities and threats, and determine which controls to implement. Risk assessment or analysis has four main steps:

Step 1. Identify assets and asset value.

Step 2. Identify vulnerabilities and threats.

Step 3. Calculate threat probability and business impact.

Step 4. Balance threat impact with countermeasure cost.

Prior to starting a risk assessment, management and the risk assessment team must determine which assets and threats to consider. This process involves determining the size of the project. The risk assessment team must then provide a report to management on the value of the assets considered. Next, management reviews and finalizes the asset list, adding and removing assets as it sees fit, and then determines the budget for the risk assessment project.

If a risk assessment is not supported and directed by senior management, it will not be successful. Management must define the purpose and scope of a risk assessment and allocate personnel, time, and monetary resources for the project.

NOTE To learn more about risk assessment, refer to Chapter 3, “Risk Mitigation Strategies and Controls.”

The statement of applicability (SOA) identifies the controls chosen by an organization and explains how and why the controls are appropriate. The SOA is derived from the output of the risk assessment. If ISO 27001 compliance is important for an organization, its SOA must directly relate the selected controls to the original risks they are intended to mitigate.

The SOA should make reference to the policies, procedures, or other documentation or systems through which the selected control will actually manifest. It is also good practice to document why controls not selected were excluded.

Business Impact Analysis (BIA)

A business impact analysis (BIA) is a functional analysis that occurs as part of business continuity and disaster recovery. Performing a thorough BIA will help business units understand the impact of a disaster. The resulting document that is produced from a BIA lists the critical and necessary business functions, their resource dependencies, and their level of criticality to the overall organization.

Interoperability Agreement (IA)

An interoperability agreement (IA) is an agreement between two or more organizations to work together to allow information exchange. The most common implementation of these agreements occurs between sister companies that are owned by the same large corporation. While the companies may be structured and managed differently, they may share systems, telecommunications, software, and data to allow consolidation and better utilization of resources. IAs are considered binding agreements.

Do not confuse an interoperability agreement with a reciprocal agreement. Whereas an IA covers normal operations, a reciprocal agreement is an agreement between two organizations that have similar technological needs and infrastructures. In a reciprocal agreement, each organization agrees to act as an alternate location for the other if the primary facilities of either of the organizations are rendered unusable. Unfortunately, in most cases, these agreements cannot be legally enforced.

Interconnection Security Agreement (ISA)

An interconnection security agreement (ISA) is an agreement between two organizations that own and operate connected IT systems to document the technical requirements of the interconnection. In most cases, the security control needs of each organization are spelled out in detail in the agreement to ensure that there is no misunderstanding. The ISA also supports a memorandum of understanding (described next) between the organizations.

For example, if an organization has completed the connection of its network to a national high-speed network, and local businesses in the area are seeking sponsorship with the organization to connect to the high-speed network by directly connecting through the organization's network, using an ISA would be the best way to document the technical requirements of the connection.

Memorandum of Understanding (MOU)

A memorandum of understanding (MOU) is an agreement between two or more organizations that details a common line of action. MOUs are often used in cases where parties either do not have a legal commitment or in situations where the parties cannot create a legally enforceable agreement. In some cases, it is referred to as a letter of intent.

Service-Level Agreement (SLA)

A service-level agreement (SLA) is an agreement about the ability of the support system to respond to problems within a certain time frame while providing an agreed level of service. SLAs can be internal between departments or external with a service provider. Agreeing on the quickness with which various problems are addressed introduces some predictability to the response to problems, which ultimately supports the maintenance of access to resources. Most service contracts are accompanied by an SLA, which may include security priorities, responsibilities, guarantees, and warranties.

For example, an SLA is the best choice when a new third-party vendor, such as a cloud computing provider, has been selected to maintain and manage an organization's systems. An SLA is also a good choice when an organization needs to provide 24-hour support for certain internal services and decides to use a third-party provider for shifts for which the organization does not have internal personnel on duty.

Operating-Level Agreement (OLA)

An operating-level agreement (OLA) is an internal organizational document that details the relationships that exist between departments to support business activities. OLAs are often used with SLAs. A good example of an OLA is an agreement between the IT department and the accounting department in which the IT department agrees to be responsible for the backup services of the accounting server, while the day-to-day operations of the accounting server are maintained by accounting personnel.

Non-Disclosure Agreement (NDA)

A non-disclosure agreement (NDA) is an agreement between two parties that defines what information is considered confidential and cannot be shared outside the two parties. An organization may implement NDAs with personnel regarding the intellectual property of the organization. NDAs can also be used when two organizations work together to develop a new product. Because certain information must be shared to make the partnership successful, NDAs are signed to ensure that each partner's data is protected.

While an NDA cannot ensure that confidential data is not shared, it usually provides details on the repercussions for the offending party, including but not limited to fines, jail time, and forfeiture of rights. For example, an organization should decide to implement an NDA when it wants to legally ensure that no sensitive information is compromised through a project with a third party or in a cloud-computing environment.

An example of an NDA in use is the one you sign when you take the CompTIA Advanced Security Practitioner exam. You must digitally sign an NDA that clearly states that you are not allowed to share any details regarding the contents of the exam except that which is expressly given in the CompTIA blueprint available on its website. Failure to comply with this NDA can result in forfeiture of your CompTIA credential and being banned from taking future CompTIA certification exams.

Business Partnership Agreement (BPA)

A business partnership agreement (BPA) is an agreement between two business partners that establishes the conditions of the partner relationship. A BPA usually includes the responsibilities of each partner, profit/loss sharing details, resource sharing details, and data sharing details.

For example, if an organization has entered into a marketing agreement with a marketing firm whereby the organization will share some of its customer information with the marketing firm, the terms should be spelled out in a BPA. The BPA should state any boundaries for the contract, such as allowing the marketing firm to only contact customers of the organization who explicitly agreed to being contacted by third parties.

BPAs should include any organizational policies that might affect the partner and its personnel. If your organization has a security policy regarding USB flash drives, any BPAs with partners that may have personnel working onsite should include the details of the USB flash drive security policy.

Master Service Agreement (MSA)

A master service agreement (MSA) is a contract between two parties in which both parties agree to most of the terms that will govern future transactions or future agreements. This agreement is ideal if an organization will have a long-term relationship with a vendor or provider. An MSA provides risk allocation strategy that outlines the risk and responsibility of contractors and employees included in the agreement for each contract's duration. It also provides indemnification that allows one party to hold harmless or safeguard another party against existing or future losses. The indemnifying party agrees to pay for damages it has caused or may cause in the future, regardless of which party is at fault; these damages include legal fees and costs associated with litigation.

An MSA usually includes a statement of work (SOW), which outlines the specific work to be executed by the vendor for the client. It includes the work activities, the deliverables, and the time line for work to be accomplished.

Security Requirements for Contracts

Contracts with third parties are a normal part of business. Because security has become such a concern for most organizations and government entities, contracts now include sections that explicitly detail the security requirements for the vendor. Organizations should consult with legal counsel to ensure that the contracts they execute include the appropriate security requirements to satisfy not only the organizations' needs but also any government regulations and laws.

Key Topic

An organization may want to consider including provisions such as the following as part of any contracts:

- Required policies, practices, and procedures related to handling organizational data
- Training or certification requirements for any third-party personnel
- Background investigation or security clearance requirements for any third-party personnel
- Required security reviews of third-party devices
- Physical security requirements for any third-party personnel
- Laws and regulations that will affect the contract

Security professionals should research security requirements for contracts, including RFPs, RFQs, RFIs, and other agreements.

Request for Proposal (RFP)

Key Topic

An RFP is a bidding-process document issued by an organization that gives details of a commodity, a service, or an asset that the organization wants to purchase. Potential suppliers use the RFP as a guideline for submitting a formal proposal.

Suppose that two members of senior management can better understand what each vendor does and what solutions they can provide after three vendors submit their requested documentation. But now the managers want to see the intricacies of how these solutions can adequately match the requirements needed by the firm. The managers should submit an RFP to the three submitting firms to obtain this information.

Request for Quote (RFQ)

Key Topic

An RFQ (sometimes called an invitation for bid [IFB]) is a bidding-process document that invites suppliers to bid on specific products or services. RFQs often include item or service specifications. An RFQ is suitable for sourcing products that are standardized or produced in repetitive quantities, such as desktop computers, RAM modules, or other devices.

Suppose that a security administrator of a small private firm is researching and putting together a proposal to purchase an intrusion prevention system (IPS). A specific brand and model has been selected, but the security administrator needs to gather cost information for that product. The security administrator should prepare an RFQ to perform a cost analysis report. The RFQ would include information such as payment terms.

Request for Information (RFI)

Key Topic

An RFI is a bidding-process document that collects written information about the capabilities of various suppliers. An RFI may be used prior to an RFP or RFQ, if needed, but can also be used after these if the RFP or RFQ does not obtain enough specification information.

Suppose that a security administrator of a large private firm is researching and putting together a proposal to purchase an IPS. The specific IPS type has not been selected, and the security administrator needs to gather information from several vendors to determine a specific product. An RFI would assist in choosing a specific brand and model.

Now let’s look at an example where the RFI comes after the RFP or RFQ. Say that three members of senior management have been working together to solicit bids for a series of firewall products for a major installation in the firm’s new office. After reviewing RFQs received from three vendors, the three managers have not gained any real data regarding the specifications about any of the solutions and want that data before the procurement continues. To get back on track in this procurement process, the managers should contact the three submitting vendor firms and have them submit supporting RFIs to provide more detailed information about their product solutions.

Agreement or Contract

Key Topic

Organizations use other types of agreements with third parties besides those already discussed. Even though many of these agreements are not as formal as RFPs, RFQs, or RFIs, it is still important for an organization to address any security requirements in an agreement to ensure that the third party is aware of the requirements. This includes any types of contracts an organization uses to perform business, including purchase orders, sales agreements, manufacturing agreements, and so on.

General Privacy Principles for Sensitive Information

When considering technology and its use today, privacy is a major concern of users. This privacy concern usually involves three areas: which personal information can be shared with whom, whether messages can be exchanged confidentially, and whether and how a user can send messages anonymously. Privacy is an integral part of an organization's security measures.

As part of the security measures that organizations must take to protect privacy, personally identifiable information (PII) must be understood, identified, and protected.

PII is any piece of data that can be used alone or with other information to identify a single person. Any PII that an organization collects must be protected in the strongest manner possible. PII includes full name, identification numbers (including driver's license number and Social Security number), date of birth, place of birth, biometric data, financial account numbers (both bank account and credit card numbers), and digital identities (including social media names and tags).

Keep in mind that different countries and levels of government can have different qualifiers for identifying PII. Security professionals must ensure that they understand international, national, state, and local regulations and laws regarding PII. As the theft of this data becomes even more prevalent, you can expect more laws to be enacted that will affect your job.

Key Topic

Figure 2-1 lists examples of PII.

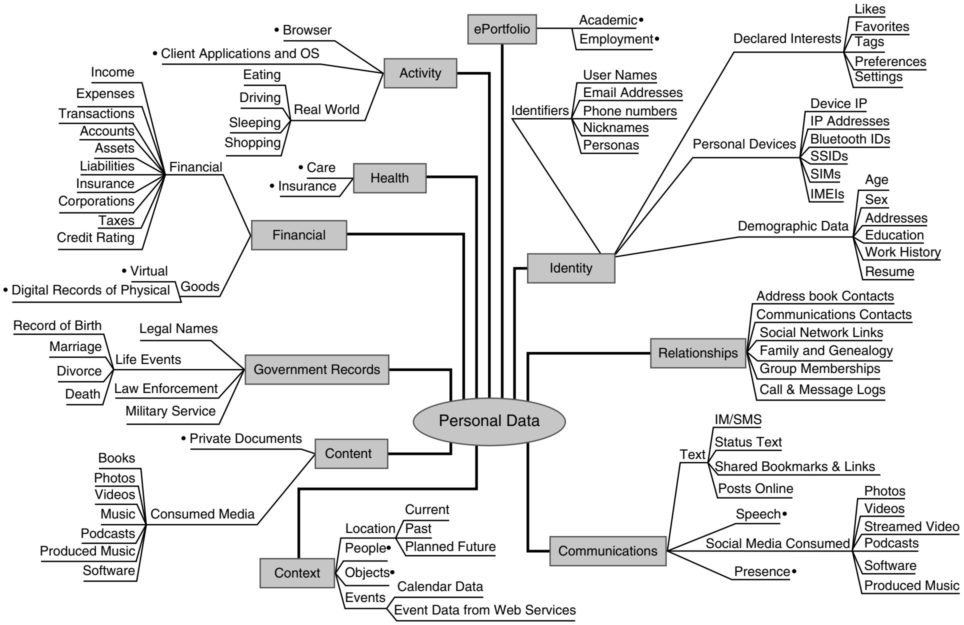

Figure 2-1 PII Examples

Support the Development of Policies Containing Standard Security Practices

Organizational policies must be implemented to support all aspects of security. Experienced security professionals should ensure that organizational security policies include separation of duties, job rotation, mandatory vacation, least privilege, incident response, forensic tasks, employment and termination procedures, continuous monitoring, training and awareness for users, and auditing requirements and frequency.

Separation of Duties

Separation of duties is a preventive administrative control to keep in mind when designing an organization's authentication and authorization policies. Separation of duties prevents fraud by distributing tasks and their associated rights and privileges among users. This helps to deter fraud and collusion because when an organization implements adequate separation of duties, collusion between two or more personnel would be required to carry out fraud against the organization. A good example of separation duties is authorizing one person to manage backup procedures and another to manage restore procedures.

Separation of duties is associated with dual controls and split knowledge. With dual controls, two or more users are authorized and required to perform certain functions. For example, a retail establishment might require two managers to open the safe. Split knowledge ensures that no single user has all the information needed to perform a particular task. An example of split knowledge is the military's requiring two individuals to each enter a unique combination to authorize missile firing.

Separation of duties ensures that one person is not capable of compromising organizational security. Any activities that are identified as high risk should be divided into individual tasks, which can then be allocated to different personnel or departments.

When an organization adopts a policy which specifies that the systems administrator cannot be present during a system audit, separation of duties is the guiding principle.

Let's look at an example of the violation of separation of duties. Say that an organization's internal audit department investigates a possible breach of security. One of the auditors interviews three employees:

- A clerk who works in the accounts receivable office and is in charge of entering data into the finance system
- An administrative assistant who works in the accounts payable office and is in charge of approving purchase orders
- The finance department manager, who can perform the functions of both the clerk and the administrative assistant

To avoid future security breaches, the auditor should suggest that the manager should only be able to review the data and approve purchase orders.

Job Rotation

From a security perspective, job rotation refers to the detective administrative control where multiple users are trained to perform the duties of a position to help prevent fraud by any individual employee. The idea is that by making multiple people familiar with the legitimate functions of the position, the likelihood increases that unusual activities by any one person will be noticed. Job rotation is often used in conjunction with mandatory vacations. Beyond the security aspects of job rotation, additional benefits include:

- Trained backup in case of emergencies
- Protection against fraud
- Cross-training of employees

Mandatory Vacation

With mandatory vacations, all personnel are required to take time off, allowing other personnel to fill their positions while gone. This detective administrative control enhances the opportunity to discover unusual activity.

Some of the security benefits of using mandatory vacations include having the replacement employee:

- Run the same applications as the vacationing employee
- Perform tasks in a different order from the vacationing employee
- Perform the job from a different workstation than the vacationing employee

Replacement employees should avoid running scripts that were created by the vacationing employee. A replacement employee should either develop his or her own script or manually complete the tasks in the script.

Least Privilege

The principle of least privilege requires that a user or process be given only the minimum access privilege needed to perform a particular task. The main purpose of this principle is to ensure that users have access to only the resources they need and are authorized to perform only the tasks they need to perform. To properly implement the least privilege principle, organizations must identify all users' jobs and restrict users to only the identified privileges.

The need-to-know principle is closely associated with the concept of least privilege. Although least privilege seeks to reduce access to a minimum, the need-to-know principle actually defines the minimums for each job or business function. Excessive privileges become a problem when a user has more rights, privileges, and permissions than needed to do his job. Excessive privileges are hard to control in large enterprise environments.

A common implementation of the least privilege and need-to-know principles is when a systems administrator is issued both an administrative-level account and a normal user account. In most day-to-day functions, the administrator should use her normal user account. When the systems administrator needs to perform administrative-level tasks, she should use the administrative-level account. If the administrator uses her administrative-level account while performing routine tasks, she risks compromising the security of the system and user accountability.

Organizational rules that support the principle of least privilege include the following:

- Keep the number of administrative accounts to a minimum.
- Administrators should use normal user accounts when performing routine operations.
- Permissions on tools that are likely to be used by attackers should be as restrictive as possible.

To more easily support the least privilege and need-to-know principles, users should be divided into groups to facilitate the confinement of information to a single group or area. This process is referred to as *compartmentalization*.

The default level of access should be no access. An organization should give users access only to resources required to do their jobs, and that access should require manual implementation after the requirement is verified by a supervisor.

Discretionary access control (DAC) and role-based access control (RBAC) are examples of systems based on a user's need to know. Ensuring least privilege requires that the user's job be identified and each user be granted the lowest clearance required for his or her tasks. Another example is the implementation of views in a database. Need-to-know requires that the operator have the minimum knowledge of the system necessary to perform his or her task.

If an administrator reviews a recent security audit and determines that two users in finance also have access to the human resource data, this could be an example of a violation of the principle of least privilege if either of the identified users works only in the finance department. Users should only be granted access to data necessary to complete their duties. While some users may require access to data outside their department, this is not the norm and should always be fully investigated.

Incident Response

Security events are inevitable. The response to an event has a great impact on how damaging the event will be to the organization. Incident response policies should be formally designed, well communicated, and followed. They should specifically address cyber attacks against an organization's IT systems.

Steps in the incident response system can include the following (see Figure 2-2):

Step 1. **Detect:** The first step is to detect the incident. All detective controls, such as auditing, discussed in Chapter 3, are designed to provide this capability. The worst sort of incident is one that goes unnoticed.

Step 2. **Respond:** The response to the incident should be appropriate for the type of incident. Denial-of-service (DoS) attacks against a web server would require a quicker and different response than a missing mouse in the server room. An organization should establish standard responses and response times ahead of time.

Step 3. **Report:** All incidents should be reported within a time frame that reflects the seriousness of the incident. In many cases, establishing a list of incident types and the person to contact when each type of incident occurs is helpful. Attention to detail at this early stage, while time-sensitive information is still available, is critical.

Step 4. **Recover:** Recovery involves a reaction designed to make the network or system affected functional again. Exactly what that means depends on the circumstances and the recovery measures that are available. For example, if fault-tolerance measures are in place, the recovery might consist of simply allowing one server in a cluster to fail over to another. In other cases, it could mean restoring the server from a recent backup. The main goal of this step is to make all resources available again.

Step 5. **Remediate:** This step involves eliminating any residual danger or damage to the network that still might exist. For example, in the case of a virus outbreak, it could mean scanning all systems to root out any additional affected machines. These measures are designed to make a more detailed mitigation when time allows.

Step 6. **Review:** The final step is to review each incident to discover what can be learned from it. Changes to procedures might be called for. It is important to share lessons learned with all personnel who might encounter the same type of incident again. Complete documentation and analysis are the goals of this step.

The actual investigation of an incident occurs during the respond, report, and recover steps. Following appropriate forensic and digital investigation processes during an investigation can help ensure that evidence is preserved.

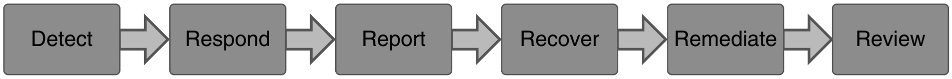

Figure 2-2 Incident Response Process

Incident response is vital to every organization to ensure that any security incidents are detected, contained, and investigated. Incident response is the beginning of any investigation. After an incident has been discovered, incident response personnel perform specific tasks. During the entire incident response, the incident response team must ensure that it follows proper procedures to ensure that evidence is preserved.

As part of incident response, security professionals must understand the difference between events and incidents. The incident response team must have the appropriate incident response procedures in place to ensure that an incident is handled, but the procedures must not hinder any forensic investigations that might be needed to ensure that parties are held responsible for any illegal actions. Security professionals must understand the rules of engagement and the authorization and scope of any incident investigation.

Events Versus Incidents

In regard to incident response, a basic difference exists between events and incidents. An event is a change of state. Whereas events include both negative and positive events, incident response focuses more on negative events—events that have been deemed to negatively impact the organization. An incident is a series of events that negatively impact an organization's operations and security. For example, an attempt to log on to the server is an event. If a system is breached because of a series of attempts to log on to the server, then an incident has occurred.

Events can be detected only if an organization has established the proper auditing and security mechanisms to monitor activity. A single negative event might occur. For example, the auditing log might show that an invalid login attempt occurred. By itself, this login attempt is not a security concern. However, if many invalid login attempts occur over a period of a few hours, the organization might be undergoing an attack. The initial invalid login is considered an event, but the series of invalid login attempts over a few hours would be an incident, especially if it is discovered that the invalid login attempts all originated from the same IP address.

Rules of Engagement, Authorization, and Scope

An organization ought to document the rules of engagement, authorization, and scope for the incident response team. The rules of engagement define which actions are acceptable and unacceptable if an incident has occurred. The authorization and scope provide the incident response team with the authority to perform an investigation and with the allowable scope of any investigation the team must undertake.

The rules of engagement act as a guideline for the incident response team to ensure that it does not cross the line from enticement into entrapment. Enticement occurs when the opportunity for illegal actions is provided (luring), but the attacker makes his own decision to perform the action. Entrapment involves encouraging someone to commit a crime that the individual might have had no intention of committing.

Enticement is legal but does raise ethical arguments and might not be admissible in court. Entrapment is illegal.

Forensic Tasks

Computer investigations require different procedures than regular investigations because the time frame for the investigator is compressed, and an expert might be required to assist in the investigation. Also, computer information is intangible and often requires extra care to ensure that the data is retained in its original format. Finally, the evidence in a computer crime can be very difficult to gather.

After a decision has been made to investigate a computer crime, you should follow standardized procedures, including the following:

- Identify what type of system is to be seized.
- Identify the search and seizure team members.
- Determine the risk of the suspect destroying evidence.

After law enforcement has been informed of a computer crime, the organization's investigator's constraints are increased. Turning over the investigation to law enforcement to ensure that evidence is preserved properly might be necessary.

When investigating a computer crime, evidentiary rules must be addressed. Computer evidence should prove a fact that is material to the case and must be reliable. The chain of custody must be maintained. Computer evidence is less likely to be admitted in court as evidence if the process for producing it has not been documented.

Key Topic

A forensic investigation involves the following steps:

Step 1. Identification

Step 2. Preservation

Step 3. Collection

Step 4. Examination

Step 5. Analysis

Step 6. Presentation

Step 7. Decision

Figure 2-3 illustrates the forensic investigation process.

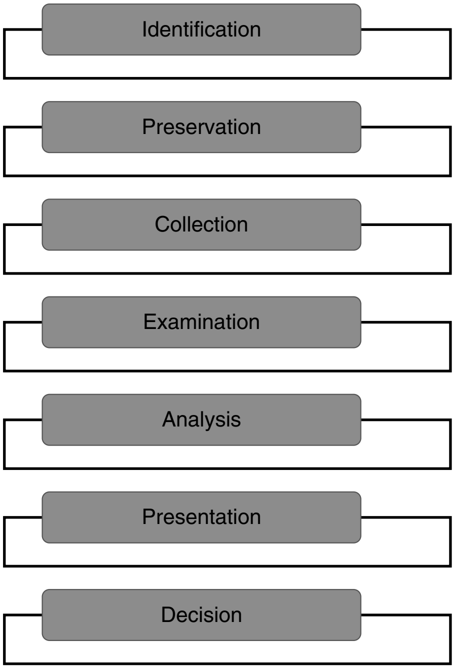

Figure 2-3 Forensic Investigation Process

Forensic investigations are discussed in more detail in Chapter 11, "Incident Response and Recovery."

Employment and Termination Procedures

Personnel are responsible for the vast majority of security issues within an organization. For this reason, it is vital that an organization implement the appropriate personnel security policies. Organizational personnel security policies should include screening, hiring, and termination policies.

Personnel screening should occur prior to the offer of employment and might include a criminal background check, work history, background investigations, credit history, driving records, substance-abuse testing, and education and licensing verification. Screening needs should be determined based on the organization's needs and the prospective hire's employment level.

Personnel hiring procedures should include signing all the appropriate documents, including government-required documentation, no expectation of privacy statements, and NDAs. An organization usually has a personnel handbook and other hiring information that must be communicated to a new employee. The hiring process should include a formal verification that the employee has completed all the training. Employee IDs and passwords are then issued.

Personnel termination must be handled differently based on whether the termination is friendly or unfriendly. Procedures defined by the human resources department can ensure that organizational property is returned, user access is removed at the appropriate time, and exit interviews are completed. With unfriendly terminations, organizational procedures must be proactive to prevent damage to organizational assets. Therefore, unfriendly termination procedures should include system and facility access termination prior to employee termination notification as well as security escort from the premises.

Management must also ensure that appropriate security policies are in place during employment. Separation of duties, mandatory vacations, and job rotation are covered earlier in this chapter. Some positions might require employment agreements to protect the organization and its assets even after the employee is no longer with the organization. These agreements can include NDAs, non-compete clauses, and code of conduct and ethics agreements.

Continuous Monitoring

Before continuous monitoring can be successful, an organization must ensure that the operational baselines are captured. After all, an organization cannot recognize abnormal patterns of behavior if it does not know what "normal" is. Periodically these baselines should also be revisited to ensure that they have not changed. For example, if a single web server is upgraded to a web server farm, a new performance baseline should be captured.

Security professionals must ensure that the organization's security posture is maintained at all times. This requires continuous monitoring. Auditing and security logs should be reviewed on a regular schedule. Performance metrics should be compared to baselines. Even simple acts such as normal user login/logout times should be monitored. If a user suddenly starts logging in and out at irregular times, the user's supervisor should be alerted to ensure that the user is authorized. Organizations must always be diligent in monitoring the security of their enterprise.

Training and Awareness for Users

Security awareness training, *security training*, and *security education* are three terms that are often used interchangeably, but these are actually three different things. Awareness training reinforces the fact that valuable resources must be protected by implementing security measures. Security training involves teaching personnel the skills they need to perform their jobs in a secure manner. Awareness training and security training are usually combined as security awareness training, which improves user awareness of security and ensures that users can be held accountable for their actions. Security education is more independent and is targeted at security professionals who require security expertise to act as in-house experts for managing security programs. So, awareness training addresses the *what*, security training addresses the *how*, and security education addresses the *why*.

Security awareness training should be developed based on the audience. In addition, trainers must understand the corporate culture and how it affects security. For example, in a small customer-focused bank, bank employees may be encouraged to develop friendships with bank clientele. In this case, security awareness training must consider the risks that come with close relationships with clients.

Key Topic

The audiences you need to consider when designing training include high-level management, middle management, technical personnel, and other staff. For high-level management, security awareness training must provide a clear understanding of potential risks and threats, effects of security issues on organizational reputation and financial standing, and any applicable laws and regulations that pertain to the organization's security program. Middle management training should discuss policies, standards, baselines, guidelines, and procedures, particularly how these components map to the individual departments. Also, middle management must understand their responsibilities regarding security. Technical staff should receive technical training on configuring and maintaining security controls, including how to recognize an attack when it occurs. In addition, technical staff should be encouraged to pursue industry certifications and higher education degrees. Other staff need to understand their responsibilities regarding security so that they perform their day-to-day tasks in a secure manner. With these staff, providing real-world examples to emphasize proper security procedures is effective.

Targeted security training is important to ensure that users at all levels understand their security duties within the organization. Let's look at an example. Say that a manager is attending an all-day training session. He is overdue on entering bonus and payroll information for subordinates and feels that the best way to get the changes entered is to log into the payroll system and activate desktop sharing with a trusted subordinate. The manager grants the subordinate control of the desktop, thereby giving the subordinate full access to the payroll system. The subordinate does not have authorization to be in the payroll system. Another employee reports the incident to the security team. The most appropriate method for dealing with this issue going forward is to provide targeted security awareness training and impose termination for repeat violators.

Personnel should sign a document indicating that they have completed the training and understand all the topics. Although the initial training should occur when someone is hired, security awareness training should be considered a continuous process, with future training sessions occurring annually at a minimum.

It is important for organizations to constantly ensure that procedures are properly followed. If an organization discovers that personnel are not following proper procedures of any kind, the organization should review the procedures to ensure that they are correct. Then the personnel should be given the appropriate training so that the proper procedures are followed.

For example, if there has been a recent security breach leading to the release of sensitive customer information, the organization must ensure that staff are trained appropriately to improve security and reduce the risk of disclosing customer data. In this case, the primary focus of the privacy compliance training program should be to explain to personnel how customer data is gathered, used, disclosed, and managed.

It is also important that security audits be performed periodically. For example, say that an organization's security audit has uncovered a lack of security controls with respect to employees' account management. Specifically, the audit reveals that accounts are not disabled in a timely manner after an employee departs the organization. The company policy states that an employee's account should be disabled within eight hours of termination. However, the audit shows that 10% of the accounts were not disabled until seven days after a dismissed employee departed. Furthermore, 5% of the accounts are still active. Security professionals should review the termination policy with the organization's managers to ensure prompt reporting of employee terminations. It may be necessary to establish a formal procedure for reporting terminations to ensure that accounts are disabled when appropriate.

Auditing Requirements and Frequency

Auditing and reporting ensure that users are held accountable for their actions, but an auditing mechanism can only report on events that it is configured to monitor. Organizations must find a balance between auditing important events and activities and ensuring that device performance is maintained at an acceptable level. Also, organizations must ensure that any monitoring that occurs is in compliance with all applicable laws.

Key Topic

Audit trails detect computer penetrations and reveal actions that identify misuse. As a security professional, you should use audit trails to review patterns of access to individual objects. To identify abnormal patterns of behavior, you should first identify normal patterns of behavior. Also, you should establish the clipping level, which is a baseline of user errors above which violations will be recorded. A common clipping level that is used is three failed login attempts. Any failed login attempt above the limit of three would be considered malicious. In most cases, a lockout policy would lock out a user's account after this clipping level was reached.

Information Classification and Life Cycle

Data should be classified based on its value to the organization and its sensitivity to disclosure. As mentioned earlier in this chapter, assigning a value to data allows an organization to determine the resources that should be used to protect the data. Resources that are used to protect data include personnel resources, monetary resources, and access control resources. Classifying data as it relates to confidentiality, integrity, and availability (CIA) allows you to apply different protective measures.

After data is classified, the data can be segmented based on the level of protection it needs. The classification levels ensure that data is handled and protected in the most cost-effective manner possible. An organization should determine the classification levels it uses based on the needs of the organization. A number of commercial business and military and government information classifications are commonly used.

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

Commercial Business Classifications

Key Topic

Commercial businesses usually classify data using four main classification levels, listed here from the highest sensitivity level to the lowest:

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

Data that is confidential includes trade secrets, intellectual data, application programming code, and other data that could seriously affect the organization if unauthorized disclosure occurred. Data at this level would be available only to personnel in the organization whose work relates to the data's subject. Access to confidential data usually requires authorization for each access. Confidential data is exempt from disclosure under the Freedom of Information Act. In most cases, the only way for external entities to have authorized access to confidential data is as follows:

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

Data that is private includes any information related to personnel—including human resources records, medical records, and salary information—that is used only within the organization. Data that is sensitive includes organizational financial information and requires extra measures to ensure its CIA and accuracy. Public data is data that would not cause a negative impact on the organization.

Military and Government Classifications

Key Topic

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

1. Top secret
2. Secret
3. Confidential
4. Sensitive but unclassified
5. Unclassified

Data that is top secret includes weapons blueprints, technology specifications, spy satellite information, and other military information that could gravely damage national security if disclosed. Data that is secret includes deployment plans, missile placement, and other information that could seriously damage national security if disclosed. Data that is confidential includes patents, trade secrets, and other information that could seriously affect the government if unauthorized disclosure occurred. Data that is sensitive but unclassified includes medical or other personal data that might not cause serious damage to national security but could cause citizens to question the reputation of the government. Military and government information that does not fall into any of the other four categories is considered unclassified and usually has to be granted to the public based on the Freedom of Information Act.

Information Life Cycle

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

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 2-1 lists these key topics and the page number on which each is found.

Key Topic

Table 2-1 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
List	Policy life cycle	66
List	Process life cycle	66
Paragraph	Risk assessment description and steps	71
List	Contract security provisions	75
Paragraph	RFP	76
Paragraph	RFQ	76
Paragraph	RFI	76
Paragraph	Agreements	77
Figure 2-1	Different types of PII	78
List	Least privilege rules	81
List	Incident response steps	81
List	Forensic investigation steps	84
Paragraph	Security awareness training audiences	87
Paragraph	Auditing guidelines	88
List	Commercial business classifications	89
List	Military and government classifications	90

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

business impact analysis (BIA), business partnership agreement (BPA), interconnection security agreement (ISA), interoperability agreement (IA), job rotation, least privilege, mandatory vacation, master service agreement (MSA), memorandum of understanding (MOU), need to know, non-disclosure agreement (NDA), operating-level agreement (OLA), personally identifiable information (PII), request for information (RFI), request for proposal (RFP), request for quote (RFQ), risk assessment, separation of duties, service-level agreement (SLA), statement of applicability (SOA)

Review Questions

1. Your organization has recently been the victim of fraud perpetrated by a single employee. After a thorough analysis has been completed of the event, security experts recommend that security controls be established to require multiple employees to complete a task. Which control should you implement, based on the expert recommendations?

    a. mandatory vacation

    b. separation of duties

    c. least privilege

    d. continuous monitoring

2. Your company has recently decided to switch Internet service providers. The new provider has provided a document that lists all the guaranteed performance levels of the new connection. Which document contains this information?

    a. SLA

    b. ISA

    c. MOU

    d. IA

3. Your organization has signed a new contract to provide database services to another company. The partner company has requested that the appropriate privacy protections be in place within your organization. Which document should be used to ensure data privacy?

   a. ISA

   b. IA

   c. NDA

   d. PII

4. Your organization has recently undergone major restructuring. During this time, a new chief security officer (CSO) was hired. He has asked you to make recommendations for the implementation of organizational security policies. Which of the following should you not recommend?

   a. All personnel are required to use their vacation time.

   b. All personnel should be cross-trained and should rotate to multiple positions throughout the year.

   c. All high-level transactions should require a minimum of two personnel to complete.

   d. The principle of least privilege should be implemented only for all high-level positions.

5. What is the primary concern of PII?

   a. availability

   b. confidentiality

   c. integrity

   d. authentication

6. Which of the following is an example of an incident?

   a. an invalid user account's login attempt

   b. account lockout for a single user account

   c. several invalid password attempts for multiple users

   d. a user attempting to access a folder to which he does not have access

7. What is the first step of a risk assessment?
   - a. Balance threat impact with countermeasure cost.
   - b. Calculate threat probability and business impact.
   - c. Identify vulnerabilities and threats.
   - d. Identify assets and asset value.

8. During a recent security audit, your organization provided the auditor with an SOA. What was the purpose of this document?
   - a. to identify the controls chosen by an organization and explain how and why the controls are appropriate
   - b. to document the performance levels that are guaranteed
   - c. to document risks
   - d. to prevent the disclosure of confidential information

9. Which document requires that a vendor reply with a formal bid proposal?
   - a. RFI
   - b. RFP
   - c. RFQ
   - d. agreement

10. Your company has decided to deploy network access control (NAC) on the enterprise to ensure that all devices comply with corporate security policies. Which of the following should be done first?
    - a. Develop the process for NAC.
    - b. Develop the procedures for NAC.
    - c. Develop the policy for NAC.
    - d. Implement NAC.

Index