TROY McMILLAN
ROBIN ABERNATHY

Cert Guide

Learn, prepare, and practice for exam success

CompTIA® Advanced Security Practitioner

CASP

CAS-002

PEARSON IT CERTIFICATION

CompTIA® Advanced Security Practitioner (CASP) CAS-002 Cert Guide

Robin Abernathy
Troy McMillan

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA® Advanced Security Practitioner (CASP) CAS-002 Cert Guide

ISBN-13: 978-0-7897-5401-1

ISBN-10: 0-7897-5401-0

Library of Congress Control Number: 2015930524

Printed in the United States of America

Second Printing: July 2015

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Allison Beaumont Johnson

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Tim Wright

Proofreader
The Wordsmithery LLC

Technical Editors
Chris Crayton
Rob Shimonski

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Lisa Matthews

Designer
Alan Clements

Composition
Tricia Bronkella

Contents at a Glance

Table of Contents

About the Authors

Robin Abernathy, CASP, is a product developer and technical editor for Kaplan IT. 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 includes practice tests and study guides for the Transcender and Self Test Software brands.

Robin most recently co-authored Pearson's *CISSP Cert Guide* with Troy McMillan. 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.

Troy McMillan, CASP, is a product developer and technical editor for Kaplan IT as well as a full-time trainer. He became a professional trainer 13 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)
- 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 and Self-Test brands. Troy lives in Sugarloaf Key, Florida, with his wife, Heike.

Dedication

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

I dedicate this book to my father, who passed away this year. I miss you every day.
—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.

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 cert prep, who have helped me to grow over the past 10 years. Thank you, Ann, George, Aima, Bob, 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 Reviewers

Chris Crayton, MCSE, is an author, technical consultant, and 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.

Rob Shimonski (www.shimonski.com) is a best-selling author and editor with over 15 years' experience developing, producing, and distributing print media in the form of books, magazines, and periodicals. To date, Rob has successfully created more than 100 books that are currently in circulation. Rob has worked for countless companies, including CompTIA, Microsoft, Pearson, Elsevier, Wiley, Cisco, the National Security Agency, and Digidesign. Rob has over 20 years' experience working in IT, networking, systems, and security. He is a veteran of the U.S. military and has been entrenched in security topics and assignments throughout his entire professional career.

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

Visit our website and register this book at www.pearsonitcertification.com/title/9780789754011 for convenient access to any updates, downloads, or errata that might be available for this book.

CompTIA

1 page Intro copy for CASP Courseware 7.22.13 v 1 1

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill.

Certification demonstrates that you have the knowledge and skill to solve technical or business problems in virtually any business environment. CompTIA certifications are highly-valued credentials that qualify you for jobs, increased compensation and promotion.

CompTIA ADVANCED SECURITY PRACTITIONER CASP

Certification Helps Your Career

- **The CompTIA Advanced Security Practitioner (CASP)** certification designates IT professionals with advanced-level security skills and knowledge.
- **The CASP** is the first mastery level certification available from CompTIA. It expands on the widely recognized path of CompTIA Security+ with almost 250,000 certified Security+ professionals.
- **Being CASP certified** demonstrates technical competency in enterprise security; risk management; research and analysis; and integration of computing, communications, and business disciplines.
- **Approved by the U.S. Department of Defense (DoD)** for 4 information assurance job roles in the DoD 8570.01-M directive: IA Technical Level III, IA Manager level II, and IA System Architect & Engineer (IASAE) Levels I and II.

Steps to Getting Certified and Staying Certified	
Review Exam Objectives	Review the Certification objectives to make sure you know what is covered in the exam. http://certification.comptia.org/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, review and answer the sample questions to get an idea what type of questions might be on the exam. http://certification.comptia.org/samplequestions.aspx
Purchase an Exam Voucher	Purchase exam vouchers on the CompTIA Marketplace. www.comptiastore.com
Take the Test	Go to the Pearson VUE website and schedule a time to take your exam. http://www.pearsonvue.com/comptia/
Stay Certified! Continuing Education	The CompTIA CASP certification is valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information go to: http://certification.comptia.org/ce

How to obtain more information

- **Visit CompTIA online:** http://certification.comptia.org/home.aspx to learn more about getting CompTIA certified.
- **Contact CompTIA:** call 866-835-8020 and choose Option 2 or email questions@comptia.org.
- **Connect with us :**

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-002 blueprint from CompTIA. This book also helps you demonstrate your knowledge by passing the CAS-002 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 defines the topics that are covered in the chapter.
- Foundation topics: At the heart of a chapter, this section explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures that build your knowledge so that you can pass the CAS-002 exam. The chapters are each broken into multiple sections.
- Key topics: This indicates 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 DVD, and in Appendix C, "Memory Tables," and Appendix D, "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 http://certification.comptia.org/getCertified/certifications/comptia-advanced-security-practitioner-(casp).

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 because of a company policy that mandates 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 CD. 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-002). 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-002 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-002 Exam Objective	CAS-002 Exam Subobjective
1 Cryptographic Concepts and Techniques	1.1 Given a scenario, select appropriate cryptographic concepts and techniques	■ Techniques ■ Concepts ■ Implementations
2 Enterprise Storage	1.2 Explain the security implications associated with enterprise storage	■ Storage types ■ Storage protocols ■ Secure storage management
3 Network and Security Components, Concepts, and Architectures	1.3 Given a scenario, analyze network and security components, concepts and architectures	■ Advanced network design (wired/wireless) ■ Security devices ■ Virtual networking and security components ■ Complex network security solutions for data flow ■ Secure configuration and baselining of networking and security components ■ Software defined networking ■ Cloud managed networks ■ Network management and monitoring tools ■ Advanced configuration of routers, switches and other network devices ■ Security zones ■ Network access control ■ Operational and consumer network enabled devices ■ Critical infrastructure/Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS)

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
4 Security Controls for Hosts	1.4 Given a scenario, select and troubleshoot security controls for hosts	■ Trusted OS (e.g., how and when to use it) ■ Endpoint security software ■ Host hardening ■ Security advantages and disadvantages of virtualizing servers ■ Cloud augmented security services ■ Boot loader protections ■ Vulnerabilities associated with co-mingling of hosts with different security requirements ■ Virtual desktop infrastructure (VDI) ■ Terminal services/application delivery services ■ TPM ■ VTPM ■ HSM
5 Application Vulnerabilities and Security Controls	1.5 Differentiate application vulnerabilities and select appropriate security controls	■ Web application security design considerations ■ Specific application issues ■ Application sandboxing ■ Application security frameworks ■ Secure coding standards ■ Database activity monitor (DAM) ■ Web application firewalls (WAFs) ■ Client-side processing vs. server-side processing
6 Business Influences and Associated Security Risks	2.1 Interpret business and industry influences and explain 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 ■ Ensuring that third party providers have requisite levels of information security ■ Internal and external influences ■ Impact of de-perimiterization (e.g., constantly changing network boundary)

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
7 Risk Mitigation Planning, Strategies, and Controls	2.2 Given a scenario, execute risk mitigation planning, strategies, and controls	■ Classify information types into levels of CIA based on organization/industry ■ Incorporate stakeholder input into CIA decisions ■ Implement technical controls based on CIA requirements and policies of the organization ■ Determine aggregate CIA scores ■ Extreme scenario planning/worst case scenario ■ Determine minimum required security controls based on the aggregate score ■ Conduct system specific risk analysis ■ Make risk determination ■ Recommend which strategy should be applied based on risk appetite ■ Risk management processes ■ Enterprise security architecture frameworks ■ Continuous improvement/monitoring ■ Business continuity planning ■ IT governance
8 Security, Privacy Policies, and Procedures	2.3 Compare and contrast security, privacy policies and procedures based on organizational requirements	■ Policy development and updates in light of new business, technology, risks and environment changes ■ Process/procedure development and updates in light of policy, environment and business changes ■ Support legal compliance and advocacy by partnering with HR, legal, management and other entities ■ Use common business documents to support security ■ Use general privacy principles for sensitive information (PII) ■ Support the development of policies

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
9 Incident Response and Recovery Procedures	2.4 Given a scenario, conduct incident response and recovery procedures	■ E-discovery ■ Data breach ■ Design systems to facilitate incident response ■ Incident and emergency response
10 Industry Trends	3.1 Apply research methods to determine industry trends and impact to the enterprise	■ Perform ongoing research ■ Situational awareness ■ Research security implications of new business tools ■ Global IA industry/community ■ Research security requirements for contracts
11 Securing the Enterprise	3.2 Analyze scenarios to secure the enterprise	■ Create benchmarks and compare to baselines ■ Prototype and test multiple solutions ■ Cost benefit analysis ■ Metrics collection and analysis ■ Analyze and interpret trend data to anticipate cyber defense needs ■ Review effectiveness of existing security controls ■ Reverse engineer/deconstruct existing solutions ■ Analyze security solution attributes to ensure they meet business needs ■ Conduct a lessons-learned/after-action report ■ Use judgment to solve difficult problems that do not have a best solution
12 Assessment Tools and Methods	3.3 Given a scenario, select methods or tools appropriate to conduct an assessment and analyze results	■ Tool type ■ Methods

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
13 Business Unit Collaboration	4.1 Given a scenario, facilitate collaboration 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 ■ IT governance
14 Secure Communication and Collaboration	4.2 Given a scenario, select the appropriate control to secure communications and collaboration solutions	■ Security of unified collaboration tools ■ Remote access ■ Mobile device management ■ Over-the-air technologies concerns
15 Security Across the Technology Life Cycle	4.3 Implement security activities across the technology life cycle	■ End-to-end solution ownership ■ Systems development life cycle ■ Adapt solutions to address emerging threats and security trends ■ Asset management (inventory control)
16 Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture	5.1 Given a scenario, integrate hosts, storage, networks and applications into a secure enterprise architecture	■ Secure data flows to meet changing business needs ■ Standards ■ Interoperability issues ■ Technical deployment models (Outsourcing/insourcing/managed services/partnership) ■ Logical deployment diagram and corresponding physical deployment diagram of all relevant devices ■ Secure infrastructure design (e.g. decide where to place certain devices/applications) ■ Storage integration (security considerations) ■ Enterprise application integration enablers

Chapter	CAS-002 Exam Objective	CAS-002 Exam Subobjective
17 Authentication and Authorization Technologies	5.2 Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives	■ Authentication ■ Authorization ■ Attestation ■ Identity propagation ■ Federation ■ Advanced trust models

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:

- Chapter 1, "Cryptographic Concepts and Techniques," introduces cryptographic techniques and concepts. It presents the uses of these techniques and describes various implementations that currently exist, such as DRM, watermarking, GPG, SSL, SSH, and S/MIME.
- Chapter 2, "Enterprise Storage," describes various types of storage mechanisms and their distinguishing characteristics. It describes the major protocols used in a storage solution and storage security and performance techniques such as multipath, snapshots, and deduplication.
- Chapter 3, "Network and Security Components, Concepts, and Architectures," covers issues driving network design, including virtual networking and security. It introduces various security devices, such as UTM, NIDS, INE, and HSM. It also includes a survey of access control issues, including network access control, and finishes with a discussion of the future of network-enabled devices, including building automation.
- Chapter 4, "Security Controls for Hosts," focuses on protecting the host in the network. Security software such as antivirus is discussed, along with the concepts and steps taken to harden systems. Security issues in a cloud environment are also covered, along with a discussion of virtual desktop security. Finally, full disk encryption is discussed.
- Chapter 5, "Application Vulnerabilities and Security Controls," discusses the fact that while securing the network is important, security issues can also exist

from the applications created by an organization. This chapter details the various problems that can be present in application code and the attacks that these problems can lead to. It also describes mitigation techniques for securing applications.

- Chapter 6, "Business Influences and Associated Security Risks," discusses the security risks involved when companies are acquired and networks are combined. This chapter introduces concepts such as security concerns when companies are merging, the risks introduced by the deperimiterization of today's networks, and the impact of outsourcing.
- As discussed in Chapter 7, "Risk Mitigation Planning, Strategies, and Controls," businesses face many types of risk in day-to-day operations. Managing risk and mitigating the damage caused by various events is the topic of this chapter. It discusses methods to use to define and quantify risk and covers methods used to select the proper strategy for handing the risks.
- As discussed in Chapter 8, "Security, Privacy Policies, and Procedures," all organizations should have security policies and procedures in place that address all conceivable events. This chapter discusses how to create a security policy and list some of the sections that should always be included.
- No security policy can protect an organization from all risks. In case a security breach occurs, there should be formal reaction system in place to address the incident. Chapter 9, "Incident Response and Recovery Procedures," describes an incident response method which ensures that evidence is protected and the proper information is gathered.
- In no industry do changes occur faster than in IT. Security professionals have to keep up with the latest practices and concept. Chapter 10, "Industry Trends," looks at some of the coming trends and methods to keep abreast of the latest and greatest security innovations and attacks.
- Chapter 11, "Securing the Enterprise," takes a more holistic security view of the enterprise and discusses how to anticipate the effects of certain security measures and how to mitigate some of these effects.
- To secure a network, you must be able to monitor the network for evidence of mischief. Chapter 12, "Assessment Tools and Methods," looks at tools used to assess the vulnerability of a network.
- Security in the network can be enhanced by all parts of the organization working together. Chapter 13, "Business Unit Collaboration," looks at the benefits of including all organizational stakeholders in the development of security policies.

- While data should be protected where it resides in storage on a network, communications crossing the network must also be secured. Chapter 14, "Secure Communication and Collaboration," looks at securing connections, both remote and local to the enterprise. It also discusses security issues surrounding collaboration tools that are now widely used.
- Security is a never-ending process that requires constant examination and adjustment. Chapter 15, "Security Across the Technology Life Cycle," covers this life cycle and also discusses change management and the benefits that can be derived from a formal change management process.
- Virtualization and cloud computing are all the rage these days. Chapter 16, "Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture," discusses the security issues involved with integrating a virtual and physical infrastructure. It covers cloud computing models and best practices for securing a virtual environment.
- Controlling access to resources and the network in general is probably the obvious security function performed by security professionals. Chapter 17, "Authentication and Authorization Technologies," covers methods of authentication and authorization.

In addition to the 17 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The CD includes practice questions that are an important part of your preparation for certification. The CD also includes a practice test and memory tables that you can work through to verify your knowledge of the subject matter.

Pearson IT Certification Practice Test Engine and Questions on the Disc

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

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

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

Install the Software from the Disc

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

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

The following steps outline the installation process:

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

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

Activate and Download the Practice Exam

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

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

2. To activate and download the exam associated with this book, from the My Products or Tools tab, select the Activate button.
3. At the next screen, enter the Activation Key from the paper inside the cardboard disc holder in the back of the book. When it's entered, click the Activate button.
4. The activation process downloads the practice exam. Click Next and then click Finish.

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

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

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

Activating Other Exams

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

Premium Edition

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

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

This page intentionally left blank

This chapter covers the following topics:

- **The Goal 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 that comprise the value of the 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 security skills and knowledge.

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 requires trained professionals that are versed not only in security theory but who can also implement measures that provide enterprisewide security. While no perquisites 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 November 30, 2014. The new exam, CAS-002, replaces CAS-001, which will retire in May 2015. This book is designed to prepare you for the new exam, CAS-002, but can also be used to prepare for the CAS-001.

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 the ability to design, implement, and maintain the correct security posture for an organization, based on the complex environments in which today's organizations exist.

Sponsoring Bodies

CompTIA is an 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 Professisonal (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, as well as 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 an unethical hacker.

Stated Goals

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

> The CASP exam covers the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments. It involves applying critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers, while managing risk.

The Value of the CASP Certification

The CASP certification holds value for both the exam candidate and the enterprise. While it is a relatively new exam, already it has been approved by U.S. Department of Defense to meet 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 one's salary

Department of Defense Directive 8570 (DoDD 8570)

DoDD 8570 prescribes 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+	GSEC	CASP
CompTIA Network+	CompTIA Security+	CISA
SSCP	SSCP	CISSP (or Associate)
		GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP	CASP	GSLC
GSLC	CAP	CISM
CompTIA Security+	GSLC	CISSP (or Associate)
	CISM	
	CISSP (or Associate)	
IASAE I	**IASAE II**	**IASAE III**
CASP	CASP	CISSP - ISSEP
CISSP (or Associate)	CISSP (or Associate)	CISSP - ISSAP

Figure I-1 DOD 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-002 exam.

1.0 Enterprise Security

1.1 Given a scenario, select appropriate cryptographic concepts and techniques

- Techniques
  - Key stretching
  - Hashing
  - Code signing
  - Pseudo random number generation
  - Perfect forward secrecy
  - Transport encryption
  - Data at rest encryption
  - Digital signature
- Concepts
  - Entropy
  - Diffusion
  - Confusion
  - Non-repudiation
  - Confidentiality
  - Integrity
  - Chain of trust, Root of trust

- Cryptographic applications and proper/improper implementations
- Advanced PKI concepts
  - Wild card
  - OCSP vs. CRL
  - Issuance to entities
  - Users
  - Systems
  - Applications
  - Key escrow
- Steganography
- Implications of cryptographic methods and design
  - Stream
  - Block
  - Modes
    - ECB
    - CBC
    - CFB
    - OFB
  - Known flaws/weaknesses
  - Strength vs. performance vs. feasibility to implement vs. interoperability

- Implementations
  - DRM
  - Watermarking
  - GPG
  - SSL
  - SSH
  - S/MIME

1.2 Explain the security implications associated with enterprise storage

- Storage types
  - Virtual storage
  - Cloud storage
  - Data warehousing
  - Data archiving
  - NAS
  - SAN
  - vSAN
- Storage protocols
  - iSCSI
  - FCoE
  - NFS, CIFS
- Secure storage management
  - Multipath
  - Snapshots
  - Deduplication
  - Dynamic disk pools
  - LUN masking/mapping
  - HBA allocation
  - Offsite or multisite replication
  - Encryption
    - Disk
    - Block
    - File
    - Record
    - Port

1.3 Given a scenario, analyze network and security components, concepts and architectures

- Advanced network design (wired/wireless)
  - Remote access
    - VPN
    - SSH
    - RDP
    - VNC
    - SSL
  - IPv6 and associated transitional technologies
  - Transport encryption
  - Network authentication methods
  - 802.1x
  - Mesh networks
- Security devices
  - UTM
  - NIPS
  - NIDS
  - INE
  - SIEM
  - HSM
  - Placement of devices
  - Application and protocol aware technologies
    - WAF
    - NextGen firewalls
    - IPS
    - Passive vulnerability scanners
    - DAM

- Virtual networking and security components
  - Switches
  - Firewalls
  - Wireless controllers
  - Routers
  - Proxies
- Complex network security solutions for data flow
  - SSL inspection
  - Network flow data
- Secure configuration and baselining of networking and security components
  - ACLs
  - Change monitoring
  - Configuration lockdown
  - Availability controls
- Software defined networking
- Cloud managed networks
- Network management and monitoring tools
- Advanced configuration of routers, switches and other network devices
  - Transport security
  - Trunking security
  - Route protection
- Security zones
  - Data flow enforcement
  - DMZ
  - Separation of critical assets
- Network access control
  - Quarantine/remediation

- Operational and consumer network enabled devices
  - Building 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)

1.4 Given a scenario, select and troubleshoot security controls for hosts

- Trusted OS (e.g. how and when to use it)
- End point security software
  - Anti-malware
  - Anti-virus
  - Anti-spyware
  - Spam filters
  - Patch management
  - HIPS/HIDS
  - Data loss prevention
  - Host-based firewalls
  - Log monitoring
- Host hardening
  - Standard operating environment/configuration baselining
    - Application whitelisting and blacklisting
  - Security/group policy implementation
  - Command shell restrictions
  - Patch management

- Configuring dedicated interfaces
  - Out-of-band NICs
  - ACLs
  - Management interface
  - Data interface
- Peripheral restrictions
  - USB
  - Bluetooth
  - Firewire
- Full disk encryption

- Security advantages and disadvantages of virtualizing servers
  - Type I
  - Type II
  - Container-based
- Cloud augmented security services
  - Hash matching
    - Anti-virus
    - Anti-spam
    - Vulnerability scanning
  - Sandboxing
  - Content filtering
- Boot loader protections
  - Secure boot
  - Measured launch
  - IMA—Integrity Measurement Architecture
  - BIOS/UEFI

- Vulnerabilities associated with co-mingling of hosts with different security requirements
  - VMEscape
  - Privilege elevation
  - Live VM migration
  - Data remnants
- Virtual Desktop Infrastructure (VDI)
- Terminal services/application delivery services
- TPM
- VTPM
- HSM

1.5 Differentiate application vulnerabilities and select appropriate security controls

- Web application security design considerations
  - Secure: by design, by default, by deployment
- Specific application issues
  - Insecure 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
- Geo-tagging
- Data remnants

- Application sandboxing
- Application security frameworks
  - Standard libraries
  - Industry accepted approaches
  - Web services security (WS-security)
- Secure coding standards
- Database Activity Monitor (DAM)
- Web Application Firewalls (WAF)
- Client-side processing vs. server-side processing
  - JSON/REST
  - Browser extensions
    - ActiveX
    - Java applets
    - Flash
  - HTML5
  - AJAX
  - SOAP
  - State management
  - Javascript

2.0 Risk Management and Incident Response

2.1 Interpret business and industry influences and explain associated security risks

- Risk management of new products, new technologies and user behaviors
- New or changing business models/strategies
  - Partnerships
  - Outsourcing
  - Cloud
  - Merger and demerger/divestiture
- Security concerns of integrating diverse industries
  - Rules
  - Policies
  - Regulations
  - Geography
- Ensuring third party providers have requisite levels of information security
- 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
  - BYOD
  - Outsourcing

2.2 Given a scenario, execute risk mitigation planning, strategies and controls

- Classify information types into levels of CIA based on organization/industry
- Incorporate stakeholder input into CIA decisions

- Implement technical controls based on CIA requirements and policies of the organization
- Determine aggregate score of CIA
- Extreme scenario planning/worst case scenario
- Determine minimum required security controls based on aggregate score
- Conduct system specific risk analysis
- Make risk determination
  - Magnitude of impact
    - ALE
    - SLE
  - Likelihood of threat
    - Motivation
    - Source
    - ARO
    - Trend analysis
  - Return on investment (ROI)
  - Total cost of ownership
- Recommend which strategy should be applied based on risk appetite
  - Avoid
  - Transfer
  - Mitigate
  - Accept
- Risk management processes
  - Exemption
  - Deterrence
  - Inherent
  - Residual
- Enterprise Security Architecture frameworks
- Continuous improvement/monitoring
- Business Continuity Planning
- IT Governance

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

- Policy development and updates in light of new business, technology, risks and environment changes
- Process/procedure development and updates in light of policy, environment and business changes
- Support legal compliance and advocacy by partnering with HR, legal, management and other entities
- Use common business documents to support security
  - Risk assessment (RA)/Statement of Applicability (SOA)
  - 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)
- Use general privacy principles for sensitive information (PII)
- Support the development of policies that contain:
  - 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

2.4 Given a scenario, conduct 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
- Design systems to facilitate incident response
  - Internal and external violations
    - Privacy policy violations
    - Criminal actions
    - Insider threat
    - Non-malicious threats/misconfigurations
  - Establish and review system, audit and security logs
- Incident and emergency response
  - Chain of custody
  - Forensic analysis of compromised system
  - Continuity of Operation Plan (COOP)
  - Order of volatility

3.0 Research, Analysis and Assessment

3.1 Apply research methods to determine industry trends and impact to the enterprise

- Perform ongoing research
  - Best practices
  - New technologies
  - New security systems and services
  - Technology evolution (e.g. RFCs, ISO)
- Situational awareness
  - Latest client-side attacks
  - Knowledge of current vulnerabilities and threats
  - Zero day mitigating controls and remediation
  - Emergent threats and issues
- Research security implications of new business tools
  - Social media/networking
  - End user cloud storage
  - Integration within the business
- Global IA industry/community
  - Computer Emergency Response Team (CERT)
  - Conventions/conferences
  - Threat actors
  - Emerging threat sources/threat intelligence
- Research security requirements for contracts
  - Request for Proposal (RFP)
  - Request for Quote (RFQ)
  - Request for Information (RFI)
  - Agreements

3.2 Analyze scenarios to secure the enterprise

- Create benchmarks and compare to baselines
- Prototype and test multiple solutions
- Cost benefit analysis
  - ROI
  - TCO
- Metrics collection and analysis
- Analyze and interpret trend data to anticipate cyber defense needs
- Review effectiveness of existing security controls
- Reverse engineer/deconstruct existing solutions
- Analyze security solution attributes to ensure they meet business needs:
  - Performance
  - Latency
  - Scalability
  - Capability
  - Usability
  - Maintainability
  - Availability
  - Recoverability
- Conduct a lessons-learned/after-action report
- Use judgment to solve difficult problems that do not have a best solution

3.3 Given a scenario, select methods or tools appropriate to conduct an assessment and analyze results

- Tool type
  - Port scanners
  - Vulnerability scanners
  - Protocol analyzer
  - Network enumerator

- Password cracker
- Fuzzer
- HTTP interceptor
- Exploitation tools/frameworks
- Passive reconnaissance and intelligence gathering tools
  - Social media
  - Whois
  - Routing tables

- Methods
  - Vulnerability assessment
  - Malware sandboxing
  - Memory dumping, runtime debugging
  - Penetration testing
  - Black box
  - White box
  - Grey box
  - Reconnaissance
  - Fingerprinting
  - Code review
  - Social engineering

4.0 Integration of Computing, Communications and Business Disciplines

4.1 Given a scenario, facilitate collaboration 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
    - 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
    - IT governance

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

- Security of unified collaboration tools
    - Web conferencing
    - Video conferencing
    - Instant messaging
    - Desktop sharing
    - Remote assistance
    - Presence
    - Email
    - Telephony
        - VoIP
    - Collaboration sites
        - Social media
        - Cloud-based
- Remote access
- Mobile device management
    - BYOD
- Over-the-air technologies concerns

4.3 Implement security activities across the technology life cycle

- End-to-end solution ownership
  - Operational activities
  - Maintenance
  - Commissioning/decommissioning
  - Asset disposal
  - Asset/object reuse
  - General change management
- Systems Development Life Cycle
  - Security System Development Life Cycle (SSDLC)/Security Development Lifecycle (SDL)
  - Security Requirements Traceability Matrix (SRTM)
  - Validation and acceptance testing
  - Security implications of agile, waterfall and spiral software development methodologies
- Adapt solutions to address emerging threats and security trends
- Asset management (inventory control)
  - Device tracking technologies
    - Geo-location/GPS location
  - Object tracking and containment technologies
    - Geo-tagging/geo-fencing
    - RFID

5.0 Technical Integration of Enterprise Components

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

- Secure data flows to meet changing business needs
- Standards
  - Open standards

- Adherence to standards
- Competing standards
- Lack of standards
- Defacto standards

- Interoperability issues
  - Legacy systems/current systems
  - Application requirements
  - In-house developed vs. commercial vs. commercial customized
- Technical deployment models (Outsourcing/insourcing/managed services/partnership)
  - Cloud and virtualization considerations and hosting options
    - Public
    - Private
    - Hybrid
    - Community
    - Multi-tenancy
    - Single tenancy
  - Vulnerabilities associated with a single physical server hosting multiple companies' virtual machines
  - Vulnerabilities associated with a single platform hosting multiple companies' virtual machines
  - Secure use of on-demand/elastic cloud computing
  - Data remnants
  - Data aggregation
  - Data isolation
  - Resources provisioning and de-provisioning
    - Users
    - Servers
    - Virtual devices
    - Applications

        - Securing virtual environments, services, applications, appliances and equipment
        - 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
    - Secure infrastructure design (e.g. decide where to place certain devices/applications)
    - Storage integration (security considerations)
    - Enterprise application integration enablers
        - CRM
        - ERP
        - GRC
        - ESB
        - SOA
        - Directory Services
        - DNS
        - CMDB
        - CMS

5.2 Given a scenario, integrate advanced authentication and authorization technologies to support enterprise objectives

- Authentication
    - Certificate-based authentication
    - Single sign-on
- Authorization
    - OAUTH
    - XACML
    - SPML

- Attestation
- Identity propagation
- Federation
  - SAML
  - OpenID
  - Shibboleth
  - WAYF
- Advanced trust models
  - RADIUS configurations
  - LDAP
  - AD

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. You can register for the exam at www.pearsonvue.com/comptia/.

About the Exam

The following are the characteristics of the exam:

- **Launches:** January 20, 2015
- **Number of questions:** 80 (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 braindumps 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-002 Blueprint, CompTIA includes a section titled "CompTIA Authorized Materials Use Policy" that details how to determine whether the materials you are using are from a legitimate company or a braindump company. This section includes a link for more information and a link to a site that will tell you if a particular provider is legitimate or a braindump, based on analysis of the content. Remember: Just because you purchase a product does not mean that the product is legitimate. Some of the best braindump companies out there charge for their products. Also, keep in mind that using materials from a braindump can result in certification revocation. Please make sure that all products you use are from a legitimate provider rather than a braindump company. Using a braindump is cheating and directly violates the nondisclosure agreement (NDA) you sign at exam time.

NOTE The following CompTIA Authorized Materials Use Policy is copied directly from the CompTIA exam blueprint. If you have any questions regarding the study materials you are considering using for this or any other CompTIA exam, please visit www.certguard.com. When you reach that site, shown in Figure I-2, simply enter the URL of the site from which materials come, and the site will tell you if the materials are authorized.

CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

Figure I-2 CompTIA Authorized Materials Use Policy

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 webpage:

http://certification.comptia.org/Training/testingcenters/policies.aspx

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 (http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

If a candidate has a question as to whether study materials are considered unauthorized (aka brain dumps), he/she should perform a search using CertGuard's engine, found here:

http://www.certguard.com/search.asp

Or verify against this list:

http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

NOTE *The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document.*

This page intentionally left blank

This chapter covers the following topics:

- **Secure Data Flows to Meet Changing Business Needs:** This section discusses security controls that can be deployed when business needs change.
- **Standards:** This section describes open standards, adherence to standards, competing standards, lack of standards, and de facto standards.
- **Interoperability Issues:** Topics covered include legacy systems/current systems, application requirements, and in-house developed versus commercial versus commercial customized applications.
- **Technical Deployment Models:** This section explains outsourcing/insourcing/managed services/partnerships, including cloud and virtualization, resource provisioning/deprovisioning, and securing and designing solutions.
- **Logical Deployment Diagram and Corresponding Physical Deployment Diagram of All Relevant Devices:** This section explains the differences between logical and physical deployment diagrams.
- **Secure Infrastructure Design:** This section gives examples of different network design models based on the network types included.
- **Storage Integration (Security Considerations):** This section lists security guidelines for integrating storage solutions.
- **Enterprise Application Integration Enablers:** This section discusses the different options available to the enterprise and when they should be deployed.

This chapter covers CASP objective 5.1.

CHAPTER 16

Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture

Organizations must securely integrate hosts, storage, networks, and applications. It is a security practitioner's responsibility to ensure that the appropriate security controls are implemented and tested. But this isn't the only step a security practitioner must take. Security practitioners must also:

- Secure data flows to meet changing business needs.
- Understand standards.
- Understand interoperability issues.
- Understand technical deployment models, including outsourcing, insourcing, managed services, and partnerships.
- Know how to segment and delegate a secure network.
- Analyze logical and physical deployment diagrams of all relevant devices.
- Design a secure infrastructure.
- Integrate secure storage solutions within the enterprise.
- Deploy enterprise application integration enablers.

All these points are discussed in detail in this chapter.

Foundation Topics

Secure Data Flows to Meet Changing Business Needs

Business needs of an organization may change and require that security devices or controls be deployed in a different manner to protect data flow. As a security practitioner, you should be able to analyze business changes, how they affect security, and then deploy the appropriate controls.

Key Topic

To protect data during transmission, security practitioners should identify confidential and private information. Once this data has been properly identified, the following analysis steps should occur:

1. Determine which applications and services access the information.
2. Document where the information is stored.
3. Document which security controls protect the stored information.
4. Determine how the information is transmitted.
5. Analyze whether authentication is used when accessing the information.
    - If it is, determine whether the authentication information is securely transmitted.
    - If it is not, determine whether authentication can be used.
6. Analyze enterprise password policies, including password length, password complexity, and password expiration.
7. Determine whether encryption is used to transmit data.
    - If it is, ensure that the level of encryption is appropriate and that the encryption algorithm is adequate.
    - If it is not, determine whether encryption can be used.
8. Ensure that the encryption keys are protected.

Security practitioners should adhere to the defense-in-depth principle to ensure that the CIA of data is ensured across its entire life cycle. Applications and services should be analyzed to determine whether more secure alternatives can be used or whether inadequate security controls are deployed. Data at rest may require encryption to provide full protection and appropriate access control lists (ACLs) to ensure that only authorized users have access. For data transmission, secure protocols and

encryption should be employed to prevent unauthorized users from being able to intercept and read data. The most secure level of authentication possible should be used in the enterprise. Appropriate password and account policies can protect against possible password attacks.

NOTE The defense-in-depth principle is further described in the introduction of this book.

Finally, security practitioners should ensure that confidential and private information is isolated from other information, including locating the information on separate physical servers and isolating data using virtual LANs (VLANs). Disable all unnecessary services, protocols, and accounts on all devices. Make sure that all firmware, operating systems, and applications are kept up-to-date, based on the vendor recommendations and releases.

When new technologies are deployed based on the changing business needs of the organization, security practitioners should be diligent to ensure that they understand all the security implications and issues with the new technology. Deploying a new technology before proper security analysis has occurred can result in security breaches that affect more than just the newly deployed technology. Remember that changes are inevitable! How you analyze and plan for these changes is what will set you apart from other security professionals.

Standards

Standards describe how policies will be implemented within an organization. They are actions or rules that are tactical in nature, meaning they provide the steps necessary to achieve security. Just like policies, standards should be regularly reviewed and revised. Standards are usually established by a governing organization, such as the National Institute of Standards and Technology (NIST).

The following sections briefly discuss open standards, adherence to standards, competing standards, lack of standards, and de facto standards.

NOTE Standards are discussed in greater detail in Chapter 5, "Application Vulnerabilities and Security Controls;" Chapter 7, "Risk Mitigation Planning, Strategies, and Controls;" Chapter 8, "Security, Privacy Policies, and Procedures;" Chapter 10, "Industry Trends;" and Chapter 15, "Security Across the Technology Life Cycle."

Open Standards

Open standards are standards that are open to the general public. The general public can provide feedback on the standards and may use the standards without purchasing any rights to the standards or organizational membership. It is important that subject matter and industry experts help guide the development and maintenance of these standards.

Adherence to Standards

Organizations may opt to adhere entirely to both open standards and those managed by a standards organization. Some organizations may even choose to adopt selected parts of standards, depending on the industry. Remember that an organization should fully review any standard and analyze how its adoption will affect the organization.

Legal implications can arise if an organization ignores well-known standards. Neglecting to use standards to guide your organization's security strategy, especially if others in your industry do, can significantly impact your organization's reputation and standing.

Competing Standards

Competing standards most often come into effect between competing vendors. For example, Microsoft often establishes its own standards for authentication. Many times, its standards are based on an industry standard with slight modifications to suit Microsoft's needs. In contrast, Linux may implement standards, but because it is an open source operating system, changes may have been made along the way that may not fully align with the standards your organization needs to follow. Always compare competing standards to determine which standard best suits your organization's needs.

Lack of Standards

In some new technology areas, standards are not formulated yet. Do not let a lack of formal standards prevent you from providing the best security controls for your organization. If you can find similar technology that has formal adopted standards, test the viability of those standards for your solution. In addition, you may want to solicit input from subject matter experts (SMEs). A lack of standards does not excuse your organization from taking every precaution necessary to protect confidential and private data.

De Facto Standards

De facto standards are standards that are widely accepted but not formally adopted. De jure standards are standards that are based on laws or regulations and are adopted by international standards organizations. De jure standards should take precedence over de facto standards. If possible, your organization should adopt security policies that implement both de facto and de jure standards.

Let's look at an example. Suppose that a chief information officer's (CIO's) main objective is to deploy a system that supports the 802.11r standard, which will help wireless VoIP devices in moving vehicles. However, the 802.11r standard has not been formally ratified. The wireless vendor's products do support 802.11r as it is currently defined. The administrators have tested the product and do not see any security or compatibility issues; however, they are concerned that the standard is not yet final. The best way to proceed would be to purchase the equipment now, as long as its firmware will be upgradable to the final 802.11r standard.

Interoperability Issues

When integrating solutions into a secure enterprise architecture, security practitioners must ensure that they understand all the interoperability issues that can occur with legacy systems/current systems, applications, and in-house versus commercial versus commercial customized applications.

Legacy Systems/Current Systems

Legacy systems are old technologies, computers, or applications that are considered outdated but provide a critical function in the enterprise. Often the vendor no longer supports the legacy systems, meaning that no future updates to the technology, computer, or application will be provided. It is always best to replace these systems as soon as possible because of the security issues they introduce. However, sometimes these systems must be retained because of the critical function they provide.

Key Topic

Some guidelines when retaining legacy systems include:

- If possible, implement the legacy system in a protected network or demilitarized zone (DMZ).
- Limit physical access to the legacy system to administrators.
- If possible, deploy the legacy application on a virtual computer.
- Employ access control lists (ACLs) to protect the data on the system.
- Deploy the highest-level authentication and encryption mechanisms possible.

Let's look at an example. Suppose an organization has a legacy customer relationship application that it needs to retain. The application requires the Windows 2000 operating system (OS), and the vendor no longer supports the application. The organization could deploy a Windows 2000 virtual machine (VM) and move the application to that VM. Users needing access to the application could use Remote Desktop to access the VM and the application.

Let's look at a more complex example. Say that an administrator replaces servers whenever budget money becomes available. Over the past several years, the

company uses 20 servers and 50 desktops from five different vendors. The management challenges and risks associated with this style of technology life cycle management include increased mean time to failure rate of legacy servers, OS variances, patch availability, and the ability to restore dissimilar hardware.

Application Requirements

Any application installed may require certain hardware, software, or other criteria that the organization does not use. However, with recent advances in virtual technology, the organization can implement a virtual machine that fulfills the criteria for the application through virtualization. For example, an application may require a certain screen resolution or graphics driver that is not available on any physical computers in the enterprise. In this case, the organization could deploy a virtual machine that includes the appropriate screen resolution or driver so that the application can be successfully deployed.

Keep in mind that some applications may require older versions of operating systems that are not available. In recent versions of Windows, you can choose to deploy an application in compatibility mode by using the Compatibility tab of the application's executable file, as shown in Figure 16-1.

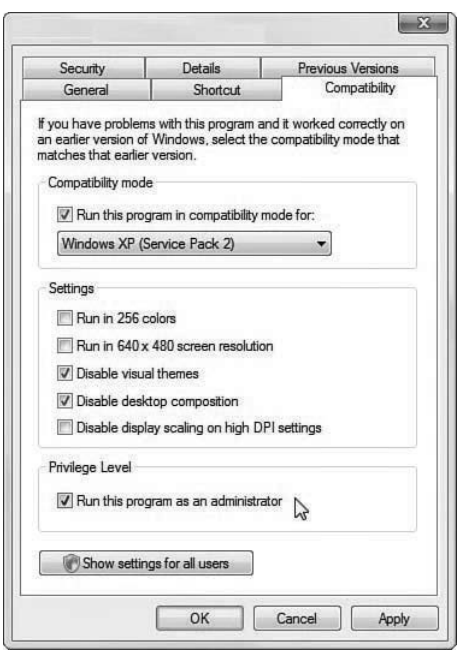

Figure 16-1 Compatibility Tab

In-House Developed Versus Commercial Versus Commercial Customized Applications

Applications can be developed in-house or purchased commercially. Applications that are developed in-house can be completely customized to the organization, provided that developers have the necessary skills, budget, and time. Commercial applications may provide customization options to the organization. However, usually the customization is limited.

Organizations should fully research their options when a new application is needed. Once an organization has documented its needs, it can compare them to all the commercially available applications to see if any of them will work. It is usually more economical to purchase a commercial solution than to develop an in-house solution. However, each organization needs to fully assess the commercial application costs versus in-house development costs.

Commercial software is well known and widely available and is commonly referred to as commercial off-the-shelf (COTS) software. Information concerning vulnerabilities and viable attack patterns is typically shared within the IT community. This means that using commercial software can introduce new security risks in the enterprise. Also, it is difficult to verify the security of commercial software code because the source is not available to customers in most cases.

NOTE For more information regarding application issues and controls, refer to Chapter 5. For more information on the systems development life cycle, refer to Chapter 15.

Technical Deployment Models

To integrate hosts, storage solutions, networks, and applications into a secure enterprise, an organization may use various technical deployment models, including outsourcing, insourcing, managed services, and partnerships. The following sections discuss cloud and virtualization considerations and hosting options, virtual machine vulnerabilities, secure use of on-demand/elastic cloud computing, data remnants, data aggregation, and data isolation.

NOTE For more information on the risks of the different business models, refer to Chapter 6, "Business Influences and Associated Security Risks."

Cloud and Virtualization Considerations and Hosting Options

Cloud computing allows enterprise assets to be deployed without the end user knowing where the physical assets are located or how they are configured. Virtualization involves creating a virtual device on a physical resource; physical resources can hold more than one virtual device. For example, you can deploy multiple virtual computers on a Windows computer. But keep in mind that each virtual machine will consume some of the resources of the host machine, and the configuration of the virtual machine cannot exceed the resources of the host machine.

For the CASP exam, you must understand public, private, hybrid, community, multi-tenancy, and single-tenancy cloud options.

NOTE For more information regarding virtualization issues, refer to Chapter 4, "Security Controls for Hosts." For more information regarding cloud issues, refer to Chapter 6.

Public Cloud

A public cloud is the standard cloud computing model, where a service provider makes resources available to the public over the Internet. Public cloud services may be free or may be offered on a pay-per-use model. An organization needs to have a business or technical liaison responsible for managing the vendor relationship but does not necessarily need a specialist in cloud deployment. Vendors of public cloud solutions include Amazon, IBM, Google, and Microsoft. In a public cloud model, subscribers can add and remove resources as needed, based on their subscription.

Private Cloud

A private cloud is a cloud computing model where a private organization implements a cloud in its internal enterprise, and that cloud is used by the organization's employees and partners. Private cloud services require an organization to employ a specialist in cloud deployment to manage the private cloud.

Hybrid Cloud

A hybrid cloud is a cloud computing model where an organization provides and manages some resources in-house and has others provided externally via a public cloud. This model requires a relationship with the service provider as well as an in-house cloud deployment specialist. Rules need to be defined to ensure that a hybrid

cloud is deployed properly. Confidential and private information should be limited to the private cloud.

Community Cloud

A community cloud is a cloud computing model where the cloud infrastructure is shared among several organizations from a specific group with common computing needs. In this model, agreements should explicitly define the security controls that will be in place to protect the data of each organization involved in the community cloud and how the cloud will be administered and managed.

Multi-Tenancy Model

A multi-tenancy model is a cloud computing model where multiple organizations share the resources. This model allows the service providers to manage the resource utilization more efficiently. In this model, organizations should ensure that their data is protected from access by other organizations or unauthorized users. In addition, organizations should ensure that the service provider will have enough resources for the future needs of the organization. If multi-tenancy models are not properly managed, one organization can consume more than its share of resources, to the detriment of the other organizations involved in the tenancy.

Single-Tenancy Model

A single-tenancy model is a cloud computing model where a single tenant uses a resource. This model ensures that the tenant organization's data is protected from other organizations. However, this model is more expensive than the multi-tenancy model.

Vulnerabilities Associated with a Single Physical Server Hosting Multiple Companies' Virtual Machines

In some virtualization deployments, a single physical server hosts multiple organizations' VMs. All of the VMs hosted on a single physical computer must share the resources of that physical server. If the physical server crashes or is compromised, all of the organizations that have VMs on that physical server are affected. User access to the VMs should be properly configured, managed, and audited. Appropriate security controls, including antivirus, antimalware, access control lists (ACLs), and auditing, must be implemented on each of the VMs to ensure that each one is properly protected. Other risks to consider include physical server resource depletion, network resource performance, and traffic filtering between virtual machines.

Driven mainly by cost, many companies outsource to cloud providers computing jobs that require a large amount of processor cycles for a short duration. This situation allows a company to avoid a large investment in computing resources that will be used for only a short time. Assuming that the provisioned resources are dedicated to a single company, the main vulnerability associated with on-demand provisioning is traces of proprietary data that can remain on the virtual machine and may be exploited.

Let's look at an example. Say that a security architect is seeking to outsource company server resources to a commercial cloud service provider. The provider under consideration has a reputation for poorly controlling physical access to data centers and has been the victim of social engineering attacks. The service provider regularly assigns VMs from multiple clients to the same physical resource. When conducting the final risk assessment, the security architect should take into consideration the likelihood that a malicious user will obtain proprietary information by gaining local access to the hypervisor platform.

Vulnerabilities Associated with a Single Platform Hosting Multiple Companies' Virtual Machines

In some virtualization deployments, a single platform hosts multiple organizations' VMs. If all of the servers that host VMs use the same platform, attackers will find it much easier to attack the other host servers once the platform is discovered. For example, if all physical servers use VMware to host VMs, any identified vulnerabilities for that platform could be used on all host computers. Other risks to consider include misconfigured platforms, separation of duties, and application of security policy to network interfaces.

If an administrator wants to virtualize the company's web servers, application servers, and database servers, the following should be done to secure the virtual host machines: only access hosts through a secure management interface and restrict physical and network access to the host console.

Secure Use of On-demand/Elastic Cloud Computing

On-demand, or elastic, cloud computing allows administrators to increase or decrease the resources utilized based on organizational needs. As demands increase, the costs increase. Therefore, it is important that resource allocation be closely monitored and managed to ensure that the organization is not paying for more resources than needed. Administrators should always use secure tools (such as Secure Shell) and encryption to connect to the host when allocating or deallocating resources.

Data Remnants

Data remnants are data that is left behind on a computer or another resource when that resource is no longer used. The best way to protect this data is to employ some sort of data encryption. If data is encrypted, it cannot be recovered without the original encryption key. If resources, especially hard drives, are reused frequently, an unauthorized user can access data remnants.

Administrators must understand the kind of data that is stored on physical drives. This helps them determine whether data remnants should be a concern. If the data stored on a drive is not private or confidential, the organization may not be concerned about data remnants. However, if the data stored on the drive is private or confidential, the organization may want to implement asset reuse and disposal policies.

NOTE For more information on asset reuse and disposal, refer to Chapter 15.

Data Aggregation

Data aggregation allows data from multiple resources to be queried and compiled together into a summary report. The account used to access the data needs to have appropriate permissions on all of the domains and servers involved. In most cases, these types of deployments will incorporate a centralized data warehousing and mining solution on a dedicated server.

Data Isolation

Data isolation in databases prevents data from being corrupted by two concurrent operations. Data isolation is used in cloud computing to ensure that tenant data in a multi-tenant solution is isolated from other tenants' data, using a tenant ID in the data labels. Trusted login services are usually used as well. In both of these deployments, data isolation should be monitored to ensure that data is not corrupted. In most cases, some sort of transaction rollback should be employed to ensure that proper recovery can be made.

Resource Provisioning and Deprovisioning

One of the benefits of many cloud deployments is the ability to provision and deprovision resources as needed. This includes provisioning and deprovisioning users, servers, virtual devices, and applications. Depending on the deployment model used, your organization may have an internal administrator that handles these tasks, the

cloud provider may handle these tasks, or you may have some hybrid solution where these tasks are split between the internal administrator and cloud provider personnel. Remember that any solution where cloud provider personnel must provide provisioning and deprovisioning may not be ideal because cloud provider personnel may not be immediately available to perform any tasks that you need.

Users

When provisioning (or creating) user accounts, it is always best to use an account template. This ensures that all of the appropriate password policies, user permissions, and other account settings are applied to the newly created account.

When deprovisioning a user account, you should consider first disabling the account. Once an account is deleted, it may be impossible to access files, folders, and other resources that are owned by that user account. If the account is disabled instead of deleted, the administrator can reenable the account temporarily to access the resources owned by that account.

An organization should adopt a formal procedure for requesting the creation, disablement, or deletion of user accounts. In addition, administrators should monitor account usage to ensure that accounts are active.

Servers

Provisioning and deprovisioning servers should be based on organizational need and performance statistics. To determine when a new server should be provisioned, administrators must monitor the current usage of the server resources. Once a predefined threshold has been reached, procedures should be put in place to ensure that new server resources are provisioned. When those resources are no longer needed, procedures should also be in place to deprovision the servers. Once again, monitoring is key.

Virtual Devices

Virtual devices consume resources of the host machine. For example, the memory on a physical machine is shared among all the virtual devices that are deployed on that physical machine. Administrators should provision new virtual devices when organizational need demands. However, it is just as important that virtual devices be deprovisioned when they are no longer needed to free up the resources for other virtual devices.

Applications

Organizations often need a variety of applications. It is important to maintain the licenses for any commercial applications that are used. When an organization no longer needs applications, administrators must be notified to ensure that licenses are not renewed or that they are renewed at a lower level if usage has simply decreased.

Securing Virtual Environments, Services, Applications, Appliances, and Equipment

When an organization deploys virtual environments, administrators and security practitioners must ensure that the virtual environments are secured in the same manner as any physical deployments of that type. For example, a virtual Windows machine needs to have the same security controls as the host server, including antivirus/antimalware software, ACLs, operating system updates, and so on. This also applies to services, applications, appliances, and equipment. You should ensure that all of the security controls are deployed as spelled out in the organization's security policies.

Design Considerations During Mergers, Acquisitions, and Demergers/Divestitures

When organizations merge, are acquired, or split, the enterprise design must be considered. In the case of mergers or acquisitions, each separate organization has its own resources, infrastructure, and model. As a security practitioner, it is important that you ensure that two organizations' structures are analyzed thoroughly before deciding how to merge them. For demergers, you probably have to help determine how to best divide the resources. The security of data should always be a top concern.

NOTE For more on the risks of these deployments, refer to Chapter 6.

Network Secure Segmentation and Delegation

An organization may need to segment its network to improve network performance, to protect certain traffic, or for a number of other reasons. Segmenting the enterprise network is usually achieved through the use of routers, switches, and firewalls. A network administrator may decide to implement VLANs using switches or deploy a demilitarized zone (DMZ) using firewalls. No matter how you choose to segment the network, you should ensure that the interfaces that connect the segments are as secure as possible. This may mean closing ports, implementing MAC filtering, and

using other security controls. In a virtualized environment, you can implement separate physical trust zones. When the segments or zones are created, you can delegate separate administrators who are responsible for managing the different segments or zones.

Logical and Physical Deployment Diagrams of Relevant Devices

Key Topic

For the CASP exam, security practitioners must understand two main types of enterprise deployment diagrams: logical deployment diagrams and physical deployment diagrams. A logical deployment diagram shows the architecture, including the domain architecture, with the existing domain hierarchy, names, and addressing scheme; server roles; and trust relationships. A physical deployment diagram shows the details of physical communication links, such as cable length, grade, and wiring paths; servers, with computer name, IP address (if static), server role, and domain membership; device location, such as printer, hub, switch, modem, router, or bridge, as well as proxy location; communication links and the available bandwidth between sites; and the number of users, including mobile users, at each site. A logical diagram usually contains less information than a physical diagram. While you can often create a logical diagram from a physical diagram, it is nearly impossible to create a physical diagram from a logical one.

An example of a logical network diagram is shown in Figure 16-2.

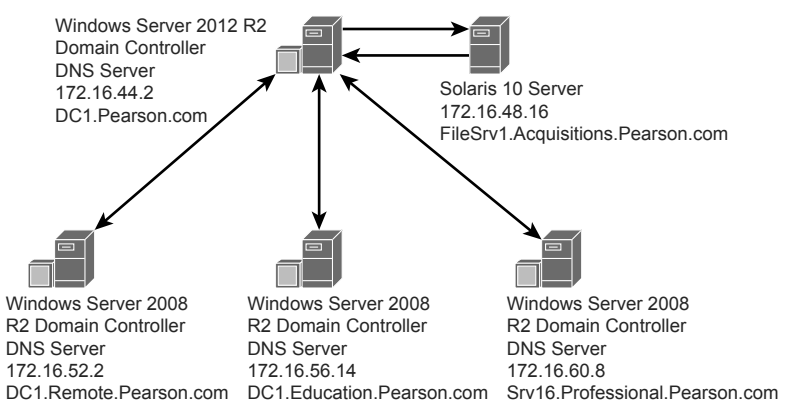

Figure 16-2 Logical Network Diagram

As you can see, the logical diagram shows only a few of the servers in the network, the services they provide, their IP addresses, and their DNS names. The relationships between the different servers are shown by the arrows between them.

An example of a physical network diagram is shown in Figure 16-3.

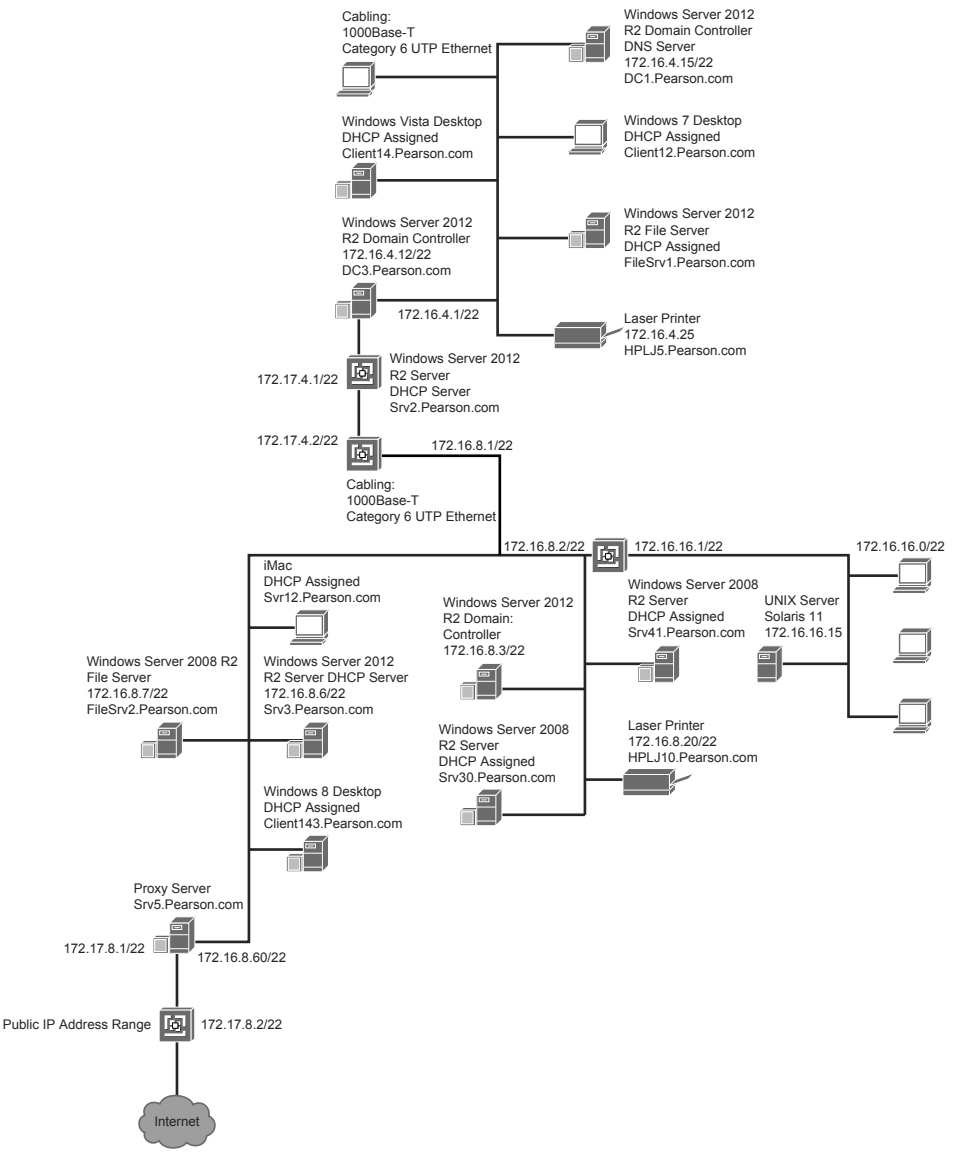

Figure 16-3 Physical Network Diagram

A physical network diagram gives much more information than a logical one, including the cabling used, the devices on the network, the pertinent information for each server, and other connection information.

Secure Infrastructure Design

As part of the CASP exam, security practitioners must be able to analyze a scenario and decide on the best placement for devices, servers, and applications. To better understand this, it is necessary to understand the different network designs that can be used. Network designs may include demilitarized zones (DMZs), VLANs, virtual private networks (VPNs), and wireless networks. This section shows examples of how these areas look. It also discusses situations in which you may need to decide where to deploy certain devices.

DMZs

A DMZ contains servers that must be accessed by the general public or partners over an Internet connection. DMZs can also be referred to as screened subnets. Placing servers on a DMZ protects the internal network from the traffic that the servers on the DMZ generate. Several examples of networks with DMZs are shown in Figure 16-4.

Key Topic

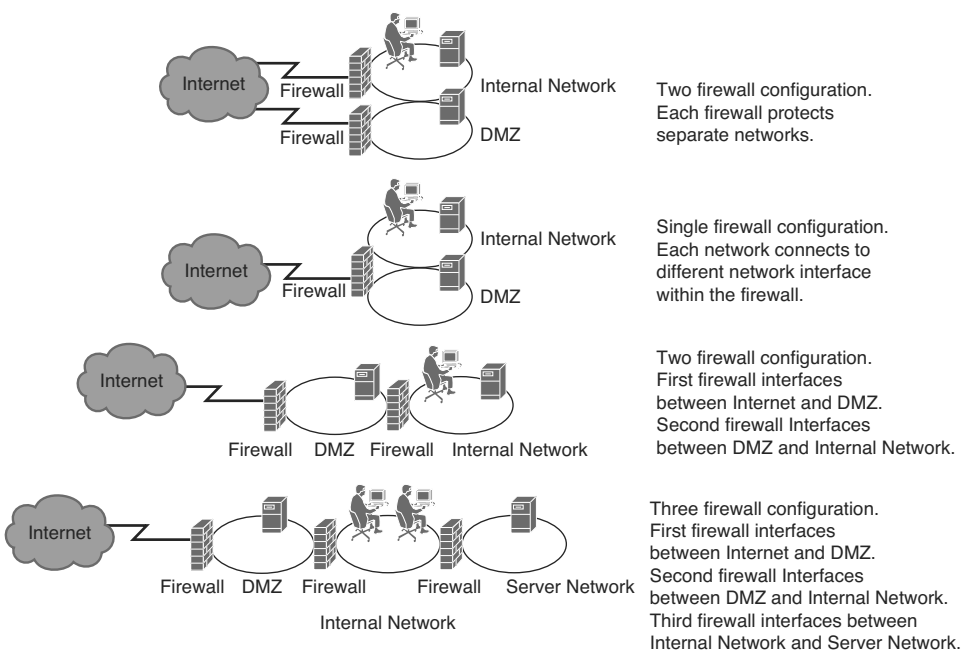

Figure 16-4 DMZ Examples

In DMZ deployments, you can configure the firewalls to allow or deny certain traffic based on a variety of settings, including IP address, MAC address, port number, or protocol. Often web servers and external-facing DNS servers are deployed on a

DMZ, with database servers and internal DNS servers being deployed on the internal network. If this is the case, then it may be necessary to configure the appropriate rules on the firewall to allow the web server to communicate with the database server and allow the external-facing DNS server to communicate with the internal DNS servers. Remember that you can also configure access rules on routers. It is important that you deploy access rules on the appropriate devices. For example, if you deny certain types of traffic on the Internet-facing router, all of that type of traffic will be unable to leave or enter the DMZ or internal network. Always analyze where the rules should be applied before creating them.

VLANs

A VLAN is a virtual network that is created using a switch. All computers and devices that are connected to a switch can be divided into separate VLANs, based on organizational needs. An example of a network with VLANs is shown in Figure 16-5.

Key Topic

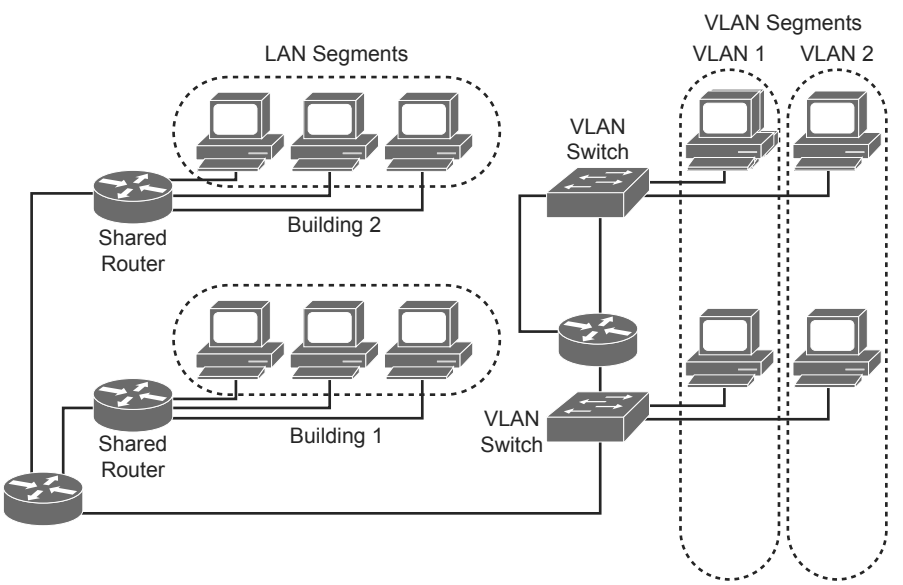

Figure 16-5 VLAN Example

In this type of deployment, each switch can have several VLANs. A single VLAN can exist on a single switch or can span multiple switches. Configuring VLANs helps manage the traffic on the switch. If you have a legacy system that is not scheduled to be decommissioned for two years and requires the use of the standard Telnet protocol, moving the system to a secure VLAN would provide the security needed until the system can be decommissioned.

VPNs

A VPN allows external devices to access an internal network by creating a tunnel over the Internet. Traffic that passes through the VPN tunnel is encrypted and protected. An example of a network with a VPN is shown in Figure 16-6.

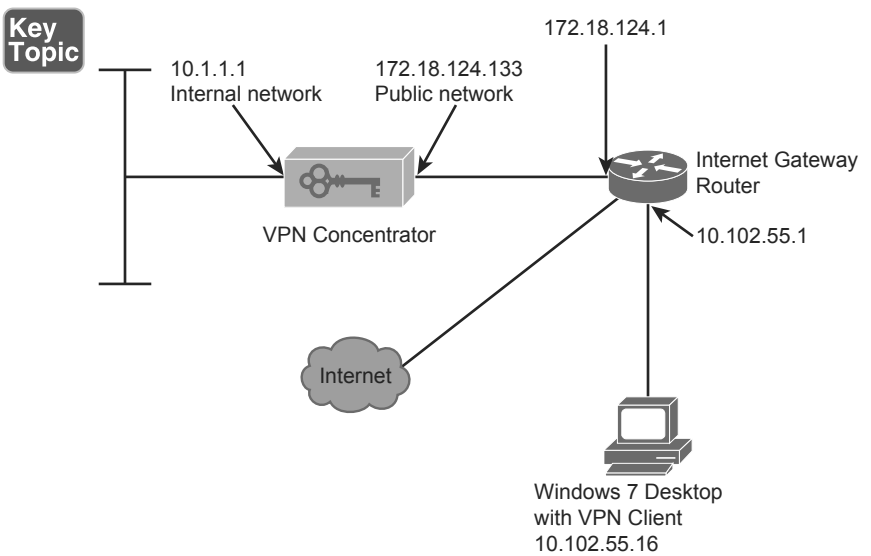

Figure 16-6 VPN Example

In a VPN deployment, only computers that have the VPN client and are able to authenticate will be able to connect to the internal resources through the VPN concentrator.

Wireless Networks

A wireless network allows devices to connect to the internal network through a wireless access point. An example of a network that includes a wireless access point is shown in Figure 16-7.

Key Topic

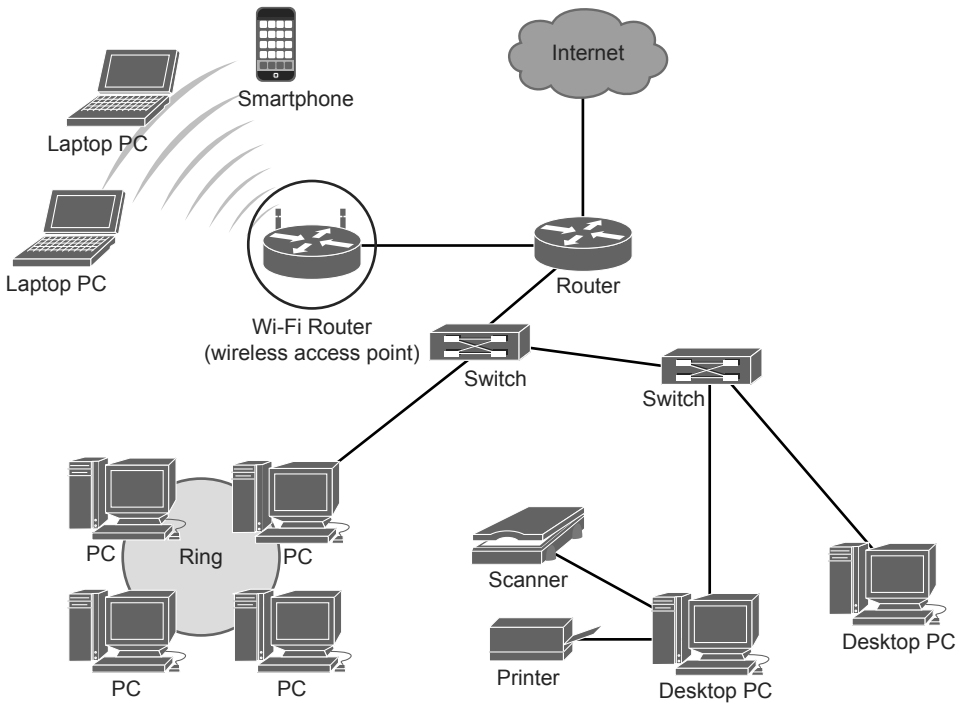

Figure 16-7 Wireless Network Example

In the deployment shown in Figure 16-7, some devices connect to the wired network, while others connect to the wireless network. The wireless network can be protected using a variety of mechanisms, including disabling the service set identifier (SSID), enabling WPA2, and implementing MAC filtering. For some organizations, it may be necessary to implement more than one wireless access point. If this occurs and all the access points use the same 802.11 implementation, then the access points will need to be configured to use different channels within that implementation. In addition, it may be necessary to adjust the signal strength of the access points to limit the coverage area.

Finally, when deciding where to place certain devices, you need to consider whether a device needs to be stored in a secured location. For example, routers, firewalls, switches, server racks, and servers are usually stored in rooms or data centers that have extra physical security controls in addition to the regular physical building security. Always consider the physical security needs when deploying any new devices.

Storage Integration (Security Considerations)

When integrating storage solutions into an enterprise, security practitioners should be involved in the design and deployment to ensure that security considerations are considered.

Key Topic

The following are some of the security considerations for storage integration that you should consider:

- Limit physical access to the storage solution.
- Create a private network to manage the storage solution.
- Implement ACLs for all data, paths, subnets, and networks.
- Implement ACLs at the port level, if possible.
- Implement multi-factor authentication.

Security practitioners should ensure that an organization adopts appropriate security policies for storage solutions to ensure that storage administrators prioritize the security of the storage solutions.

Enterprise Application Integration Enablers

Enterprise application integration enablers ensure that applications and services in an enterprise are able to communicate as needed. For the CASP exam, the primary concerns are understanding which enabler is needed in a particular situation or scenario and ensuring that the solution is deployed in the most secure manner possible. The solutions that you must understand include customer relationship management (CRM); enterprise resource planning (ERP); governance, risk, and compliance (GRC); enterprise service bus (ESB); service-oriented architecture (SOA); Directory Services; Domain Name System (DNS); configuration management database (CMDB); and content management systems (CMSs).

CRM

Customer relationship management (CRM) identifies customers and stores all customer-related data, particularly contact information and data on any direct contacts with customers. The security of CRM is vital to an organization. In most cases, access to the CRM is limited to sales and marketing personnel and management. If remote access to CRM is required, you should deploy a VPN or similar solution to ensure that the CRM data is protected.

ERP

Enterprise resource planning (ERP) collects, stores, manages, and interprets data from product planning, product cost, manufacturing or service delivery, marketing/sales, inventory management, shipping, payment, and any other business processes. ERP is accessed by personnel for reporting purposes. ERP should be deployed on a secured internal network or DMZ. When deploying ERP, you might face objections because some departments may not want to share their process information with other departments.

GRC

Governance, risk, and compliance (GRC) coordinates information and activity across these three areas to be more efficient, to enable information sharing and reporting, and to avoid waste. This integration improves the overall security posture of any organization. However, the information stored in GRC is tied closely to the organization's security. Access to this system should be tightly controlled.

ESB

Enterprise service bus (ESB) designs and implements communication between mutually interacting software applications in a service-oriented architecture (SOA). It allows SOAP, Java, .NET, and other applications to communicate. An ESB solution is usually deployed on a DMZ to allow communication with business partners.

ESB is the most suitable solution for providing event-driven and standards-based secure software architecture.

SOA

Service-oriented architecture (SOA) uses software pieces to provide application functionality as services to other applications. A service is a single unit of functionality. Services are combined to provide the entire functionality needed. This architecture often intersects with web services.

Let's look at an SOA scenario. Suppose a database team suggests deploying an SOA-based system across the enterprise. The chief information officer (CIO) decides to consult the security manager about the risk implications for adopting this architecture. The security manager should present to the CIO two concerns for the SOA system: Users and services are distributed, often over the Internet, and SOA abstracts legacy systems such as web services, which are often exposed to outside threats.

Directory Services

Directory Services stores, organizes, and provides access to information in a computer operating system's directory. With Directory Services, users can access a resource by using the resource's name instead of its IP or MAC address. Most enterprises implement an internal Directory Services server that handles any internal requests. This internal server communicates with a root server on a public network or with an externally facing server that is protected by a firewall or other security device to obtain information on any resources that are not on the local enterprise network. Active Directory, DNS, and LDAP are examples of directory services.

DNS

Domain Name System (DNS) provides a hierarchical naming system for computers, services, and any resources connected to the Internet or a private network. You should enable Domain Name System Security Extensions (DNSSEC) to ensure that a DNS server is authenticated before the transfer of DNS information begins between the DNS server and client. Transaction Signature (TSIG) is a cryptographic mechanism used with DNSSEC that allows a DNS server to automatically update client resource records if their IP addresses or hostnames change. The TSIG record is used to validate a DNS client.

As a security measure, you can configure internal DNS servers to communicate only with root servers. When you configure internal DNS servers to communicate only with root servers, the internal DNS servers are prevented from communicating with any other external DNS servers.

The Start of Authority (SOA) contains the information regarding a DNS zone's authoritative server. A DNS record's Time to Live (TTL) determines how long a DNS record will live before it needs to be refreshed. When a record's TTL expires, the record is removed from the DNS cache. Poisoning the DNS cache involves adding false records to the DNS zone. If you use a longer TTL, the resource record is read less frequently and therefore is less likely to be poisoned.

Let's look at a security issue that involves DNS. An IT administrator installs new DNS name servers that host the company mail exchanger (MX) records and resolve the web server's public address. To secure the zone transfer between the DNS servers, the administrator uses only server ACLs. However, any secondary DNS servers would still be susceptible to IP spoofing attacks.

Another scenario could occur when a security team determines that someone from outside the organization has obtained sensitive information about the internal organization by querying the company's external DNS server. The security manager should address the problem by implementing a split DNS server, allowing the external DNS server to contain only information about domains that the outside world

should be aware and the internal DNS server to maintain authoritative records for internal systems.

CMDB

A configuration management database (CMDB) keeps track of the state of assets, such as products, systems, software, facilities, and people, as they exist at specific points in time, as well as the relationships between such assets. The IT department typically uses CMDBs as data warehouses.

CMS

A content management system (CMS) publishes, edits, modifies, organizes, deletes, and maintains content from a central interface. This central interface allows users to quickly locate content. Because edits occur from this central location, it is easy for users to view the latest version of the content. Microsoft SharePoint is an example of a CMS.

Exam Preparation Tasks

You have a couple of choices for exam preparation: the exercises here and the exam simulation questions on the CD-ROM.

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 16-1 lists these key topics and the page number on which each is found.

Key Topic

Table 16-1 Key Topics for Chapter 16

Key Topic Element	Description	Page Number
Paragraph/numbered list	Secure data flow steps	534
Bulleted list	Legacy system guidelines	537
Paragraph	Logical versus physical deployment models	546
Figure 16-4	DMZ example	548
Figure 16-5	VLAN example	549
Figure 16-6	VPN example	550
Figure 16-7	Wireless example	551
Bulleted list	Storage integration security considerations	552

Define Key Terms

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

open standards; de facto standards; de jure standards; legacy system; public cloud; private cloud; hybrid cloud; community cloud; multi-tenancy cloud model; single-tenancy cloud model; data remnants; data aggregation; data isolation; logical deployment diagram; physical deployment diagram; customer relationship management (CRM); enterprise resource planning (ERP); governance, risk, and compliance (GRC), enterprise service bus (ESB); service-oriented architecture (SOA); directory services; Domain Name System (DNS); configuration management database (CMDB); content management system (CMS)

Review Questions

1. Several business changes have occurred in your company over the past six months. You must analyze your enterprise's data to ensure that data flows are protected. Which of the following guidelines should you follow? (Choose all that apply.)
   a. Determine which applications and services access the data.
   b. Determine where the data is stored.
   c. Share encryption keys with all users.
   d. Determine how the data is transmitted.

2. During a recent security analysis, you determine that users do not use authentication when accessing some private data. What should you do first?
   a. Encrypt the data.
   b. Configure the appropriate ACL for the data.
   c. Determine whether authentication can be used.
   d. Implement complex user passwords.

3. Your organization must comply with several industry and governmental standards to protect private and confidential information. You must analyze which standards to implement. Which standards should you consider?
   a. open standards, de facto standards, and de jure standards
   b. open standards only
   c. de facto standards only
   d. de jure standards only

4. Your organization has recently experienced issues with data storage. The servers you currently use do not provide adequate storage. After researching the issues and the options available, you decide that data storage needs for your organization will grow exponentially over the new couple years. However, within three years, data storage needs will return to the current demand. Management wants to implement a solution that will provide for the current and future needs without investing in hardware that will no longer be needed in the future. Which recommendation should you make?
   a. Deploy virtual servers on the existing machines.
   b. Contract with a public cloud service provider.
   c. Deploy a private cloud service.
   d. Deploy a community cloud service.

5. Management expresses concerns about using multi-tenant public cloud solutions to store organizational data. You explain that tenant data in a multi-tenant solution is quarantined from other tenants' data using a tenant ID in the data labels. What is this condition referred to?
   a. data remnants
   b. data aggregation
   c. data purging
   d. data isolation

6. You have been hired as a security practitioner for an organization. You ask the network administrator for any network diagrams that are available. Which network diagram would give you the most information?
   a. logical network diagram
   b. wireless network diagram
   c. physical network diagram
   d. DMZ diagram

7. Your organization has recently partnered with another organization. The partner organization needs access to certain resources. Management wants you to create a perimeter network that contains only the resources that the partner organization needs to access. What should you do?
   a. Deploy a DMZ.
   b. Deploy a VLAN.
   c. Deploy a wireless network.
   d. Deploy a VPN.

8. Your organization has recently started allowing sales people to access internal resources remotely. Management wants you to configure the appropriate controls to provide maximum security for these connections. What should you do?
   a. Deploy a DMZ.
   b. Deploy a VLAN.
   c. Deploy a wireless network.
   d. Deploy a VPN.

9. Recently, sales people within your organization are having trouble managing customer-related data. Management is concerned that sales figures are being negatively affected as a result of this mismanagement. You have been asked to provide a suggestion to fix this problem. What should you recommend?
   a. Deploy an ERP solution.
   b. Deploy a CRM solution.
   c. Deploy a GRC solution.
   d. Deploy a CMS solution.

10. As your enterprise has grown, it has become increasingly hard to access and manage resources. Users often have trouble locating printers, servers, and other resources. You have been asked to deploy a solution that will allow easy access to internal resources. Which solution should you deploy?
   a. Directory Services
   b. CMDB
   c. ESB
   d. SOA

This page intentionally left blank

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y-Z