

Michael Gregg and Billy Haines

CASP

CompTIA® Advanced Security Practitioner STUDY GUIDE



AUTHORIZED

EXAM CAS-001

Includes Real-World Scenarios, Lab Exercises,
and Access to Exam Prep Software Featuring:

- + Custom Test Engine
- + Hundreds of Practice Questions
- + Electronic Flashcards



SERIOUS SKILLS.

CASP

CompTIA® Advanced Security Practitioner

Study Guide



CASP

CompTIA® Advanced Security Practitioner

Study Guide



Michael Gregg
Billy Haines



John Wiley & Sons, Inc.

Senior Acquisitions Editor: Jeff Kellum
Development Editor: Dick Margulis
Technical Editors: Shawn Merdinger and Billy Haines
Production Editor: Eric Charbonneau
Copy Editor: Liz Welch
Editorial Manager: Pete Gaughan
Production Manager: Tim Tate
Vice President and Executive Group Publisher: Richard Swadley
Vice President and Publisher: Neil Edde
Media Project Manager 1: Laura Moss-Hollister
Media Associate Producer: Josh Frank
Media Quality Assurance: Marilyn Hummel
Book Designer: Judy Fung
Compositor: Craig Woods, Happenstance Type-O-Rama
Proofreader: Jen Larsen, Word One New York
Indexer: Ted Laux
Project Coordinator, Cover: Katherine Crocker
Cover Designer: Ryan Sneed

Copyright © 2012 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-118-08319-2 (pbk)

ISBN: 978-1-118-22272-0 (ebk)

ISBN: 978-1-118-23661-1 (ebk)

ISBN: 978-1-118-26152-1 (ebk)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Not all content that is available in standard print versions of this book may appear or be packaged in all book formats. If you have purchased a version of this book that did not include media that is referenced by or accompanies a standard print version, you may request this media by visiting <http://booksupport.wiley.com>. For more information about Wiley products, visit us at www.wiley.com.

Library of Congress Control Number: 2011945563

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. CompTIA is a registered trademark of Computing Technology Industry Association, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *CASP: CompTIA Advanced Security Practitioner Study Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at nedde@wiley.com. If you think you've found a technical error in this book, please visit <http://sybex.custhelp.com>. Customer feedback is critical to our efforts at Sybex.

Best regards,

A handwritten signature in black ink, appearing to read 'Neil Edde', with a stylized, flowing script.

Neil Edde
Vice President and Publisher
Sybex, an Imprint of Wiley

To Christine, thank you for your love and for always supporting me in my endeavors.

I love you.

—Michael Gregg

I would like to dedicate this, my first book, to God, my beloved wife Jackie, my son John, my parents and grandparents Bill and Jeannette and Bill and Bettie respectively, and finally to my Uncle Cliff.

—Billy Haines

Acknowledgments

I want to acknowledge and thank the talented team at Sybex and Wiley for their tireless pursuit of accuracy, precision, and clarity. Thank you for your skillful efforts.

I would also like to acknowledge and thank you, the reader, for your desire for self-improvement and your faith in us to produce a resource worthy of your time, money, and consumption. We've done our best to make this a powerful asset in your efforts to be a better IT professional. To all of you who read this book, keep learning and taking steps to move your career forward.

—*Michael Gregg*

First I would like to acknowledge the Sybex team—Pete, Jeff, Liz, and Eric; Michael Gregg for giving me the opportunity; Mary Purdy with BAH for pushing ever-so-gently in the direction of the CASP; my Warrant CWO3 Walter Moss for pushing me not-so-gently in every other direction; my Commanding Officer CDR Matthew Rick for his recognition and sheer patriotism; Adam Liss of Google for recommending the Google Authors conference among many other things; and finally Rickey Jackson for his BackTrack support and externally facing X-Windows: no, I will never let you live that one down.

—*Billy Haines*

About the Authors

Michael Gregg is the founder and president of Superior Solutions, Inc., a Houston, Texas–based IT security consulting firm. Superior Solutions performs security assessments and penetration testing for Fortune 1000 firms. The company has performed security assessments for private, public, and governmental agencies. Its Houston-based team travels the United States to assess, audit, and provide training services.

Michael is responsible for working with organizations to develop cost-effective and innovative technology solutions to security issues and for evaluating emerging technologies. He has more than 20 years of experience in the IT field and holds two associate's degrees, a bachelor's degree, and a master's degree. In addition to co-writing the first, second, and third editions of *Security Administrator Street Smarts*, Michael has written or co-written 14 other books, including *Build Your Own Security Lab: A Field Guide for Network Testing* (ISBN: 978-0470179864), *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network* (ISBN: 978-1597491099), *Certified Ethical Hacker Exam Prep 2* (ISBN: 978-0789735317), and *Inside Network Security Assessment: Guarding Your IT Infrastructure* (ISBN: 978-0672328091).

Michael has created over a dozen training security classes and training manuals and is the author of the only officially approved third-party Certified Ethical Hacker training material. He has created and performed video instruction on many security topics such as Cyber Security, CISSP, CISA, Security+, and others.

When not consulting, teaching, or writing, Michael enjoys 1960s muscle cars and giving back to the community. He is a board member for Habitat for Humanity.

Billy Haines is a computer hobbyist/security enthusiast. He served six years in the United States Navy and has visited 19 countries. He currently possesses various certifications, including the CCNA Security and CISSP Associate. His home lab consists of a variety of Cisco equipment ranging from 1841 routers to 3550 and 3560 switches. He runs a myriad of operating systems, including Debian Linux and OpenBSD, and has served as the technical editor for a variety of security-related publications. He can be reached at billy.haines@hushmail.com.

Contents at a Glance

<i>Foreword</i>		<i>xxi</i>
<i>Introduction</i>		<i>xxvii</i>
<i>Assessment Test</i>		<i>xliv</i>
Chapter 1	Cryptographic Tools and Techniques	1
Chapter 2	Comprehensive Security Solutions	37
Chapter 3	Securing Virtualized, Distributed, and Shared Computing	77
Chapter 4	Host Security	109
Chapter 5	Application Security and Penetration Testing	145
Chapter 6	Risk Management	189
Chapter 7	Policies, Procedures, and Incident Response	229
Chapter 8	Security Research and Analysis	263
Chapter 9	Enterprise Security Integration	311
Chapter 10	Security Controls for Communication and Collaboration	343
Appendix A	CASP Lab Manual	385
Appendix B	Answers to Review Questions	463
Appendix C	About the Additional Study Tools	475
<i>Index</i>		<i>479</i>

Contents

<i>Foreword</i>	<i>xxi</i>
<i>Introduction</i>	<i>xxvii</i>
<i>Assessment Test</i>	<i>xliv</i>

Chapter 1	Cryptographic Tools and Techniques	1
	The History of Cryptography	2
	Cryptographic Services	3
	Cryptographic Goals	3
	Cryptographic Terms	4
	Cipher Types and Methods	6
	Symmetric Encryption	8
	Data Encryption Standard	10
	Triple-DES	11
	Advanced Encryption Standard	12
	International Data Encryption Algorithm	12
	Rivest Cipher Algorithms	13
	Asymmetric Encryption	13
	Diffie–Hellman	14
	RSA	15
	Elliptic Curve Cryptography	16
	El Gamal	16
	Merkle–Hellman Knapsack	16
	Hybrid Encryption	16
	Hashing	17
	Hashing and Message Digests	17
	MD Series	19
	SHA	19
	HAVAL	19
	Message Authentication Code	20
	HMAC	20
	Digital Signatures	20
	Public Key Infrastructure	22
	Certificate Authority	22
	Registration Authority	23
	Certificate Revocation List	23
	Digital Certificates	24
	Certificate Distribution	26
	The Client’s Role in PKI	26
	Cryptographic Solutions	27
	Application Layer Encryption	27
	Transport Layer Encryption	28

	Internet Layer Controls	28
	Physical Layer Controls	29
	Cryptographic Attacks	30
	Summary	31
	Exam Essentials	31
	Review Questions	33
Chapter 2	Comprehensive Security Solutions	37
	Advanced Network Design	39
	Remote Access	40
	Placement of Security Devices	41
	SCADA	44
	VoIP	45
	TCP/IP	47
	Network Interface Layer	48
	Internet Layer	50
	Transport Layer	55
	Application Layer	57
	Secure Communication Solutions	60
	Secure Facility Solutions	66
	Building Layouts	66
	Facilities Management	67
	Secure Network Infrastructure Design	67
	Router Configuration	68
	Enterprise Service Bus	69
	Web Services Security	70
	Summary	70
	Exam Essentials	71
	Review Questions	73
Chapter 3	Securing Virtualized, Distributed, and Shared Computing	77
	Enterprise Security	79
	Cloud Computing	81
	Cloud Computing Models	82
	Cloud Computing Providers	83
	Benefits of Cloud Computing	83
	Security of Cloud Computing	86
	Cloud Computing Vulnerabilities	90
	Virtualization	92
	Virtualized Servers	93
	Virtual LANs	97
	Enterprise Storage	98
	Summary	103

	Exam Essentials	103
	Review Questions	105
Chapter 4	Host Security	109
	Firewalls and Access Control Lists	110
	Host-Based Firewalls	114
	Trusted Operating System	117
	Endpoint Security Software	121
	Anti-malware	124
	Antivirus	124
	Anti-spyware	126
	Spam Filters	128
	Host Hardening	129
	Asset Management	133
	Data Exfiltration	134
	Intrusion Detection and Prevention	135
	Summary	139
	Exam Essentials	139
	Review Questions	141
Chapter 5	Application Security and Penetration Testing	145
	Application Security	147
	Specific Application Issues	149
	Cross-Site Scripting	150
	Clickjacking	151
	Session Management	151
	Input Validation	152
	SQL Injection	153
	Application Sandboxing	154
	Application Security Framework	154
	Standard Libraries	155
	Secure Coding Standards	156
	Application Exploits	157
	Escalation of Privilege	158
	Improper Storage of Sensitive Data	159
	Cookie Storage and Transmission	159
	Process Handling at the Client and Server	160
	Ajax	161
	JavaScript	161
	Buffer Overflow	162
	Memory Leaks	163
	Integer Overflow	163
	Race Conditions (TOC/TOU)	163
	Resource Exhaustion	164

	Security Assessments and Penetration Testing	165
	Test Methods	166
	Penetration Testing Steps	166
	Assessment Types	167
	Assessment Areas	168
	Security Assessment and Penetration Test Tools	170
	Summary	182
	Exam Essentials	182
	Review Questions	184
Chapter 6	Risk Management	189
	Risk Terminology	191
	Identifying Vulnerabilities	192
	Operational Risks	195
	Risk in Business Models	195
	Risk in External and Internal Influences	201
	Risks with Data	204
	The Risk Assessment Process	210
	Asset Identification	210
	Information Classification	212
	Risk Assessment	213
	Risk Analysis Options	217
	Implementing Controls	218
	Continuous Monitoring	219
	Enterprise Security Architecture Frameworks	220
	Best Practices for Risk Assessments	220
	Summary	221
	Exam Essentials	222
	Review Questions	224
Chapter 7	Policies, Procedures, and Incident Response	229
	A High-Level View of Documentation	231
	The Policy Development Process	232
	Policies and Procedures	233
	Business Documents Used to Support Security	237
	Documents and Controls Used for Sensitive Information	239
	Why Security?	240
	Personally Identifiable Information Controls	240
	Data Breach	242
	Policies Used to Manage Employees	243
	Auditing Requirements and Frequency	247
	The Incident Response Framework	248
	Digital Forensics	250
	The Role of Training and Employee Awareness	254

	Summary	255
	Exam Essentials	256
	Review Questions	258
Chapter 8	Security Research and Analysis	263
	Analyzing Industry Trends and Outlining Potential Impact	266
	Performing Ongoing Research	266
	Best Practices	270
	New Technologies	273
	Situational Awareness	281
	Research Security Implications of New Business Tools	290
	Global IA Industry Community	293
	Research Security Requirements for Contracts	296
	Carrying Out Relevant Analysis to Secure the Enterprise	298
	Benchmarking	298
	Prototyping and Testing Multiple Solutions	298
	Cost-Benefit Analysis	299
	Analyzing and Interpreting Trend Data to	
	Anticipate Cyber Defense Aids	299
	Reviewing Effectiveness of Existing Security	299
	Reverse Engineering or Deconstructing Existing Solutions	301
	Analyzing Security Solutions to Ensure They	
	Meet Business Needs	301
	Conducting a Lessons Learned/After-Action Review	302
	Using Judgment to Solve Difficult Problems	303
	Conducting Network Traffic Analysis	303
	Summary	304
	Exam Essentials	305
	Review Questions	306
Chapter 9	Enterprise Security Integration	311
	Integrate Enterprise Disciplines to Achieve Secure Solutions	313
	The Role of Governance in Achieving Enterprise Security	315
	Interpreting Security Requirements and Goals	
	to Communicate with Other Disciplines	317
	Guidance to Management	320
	Establish Effective Collaboration within Teams	
	to Implement Secure Solutions	322
	Disciplines	325
	Explain the Security Impact of Interorganizational Change	328
	Security Concerns of Interconnecting Multiple Industries	330
	Design Considerations During Mergers,	
	Acquisitions, and De-mergers	331

	Assuring Third-Party Products Only Introduce Acceptable Risk	332
	Network Secure Segmentation and Delegation	334
	Integration of Products and Services	336
	Summary	337
	Exam Essentials	338
	Review Questions	339
Chapter 10	Security Controls for Communication and Collaboration	343
	Selecting and Distinguishing the Appropriate Security Controls	345
	Unified Communication Security	345
	VoIP Security	354
	VoIP Implementation	356
	Remote Access	357
	Enterprise Configuration Management of Mobile Devices	358
	Secure External Communications	359
	Secure Implementation of Collaboration Platforms	360
	Prioritizing Traffic with QoS	362
	Mobile Devices	363
	Advanced Authentication Tools, Techniques, and Concepts	365
	Federated Identity Management	365
	XACML	366
	SOAP	366
	SSO	367
	Service Provisioning Markup Language	368
	Certificate-Based Authentication	369
	Carrying Out Security Activities across the Technology Life Cycle	370
	End-to-End Solution Ownership	370
	Understanding the Results of Solutions in Advance	371
	Systems Development Life Cycle	373
	Addressing Emerging Threats and Security Trends	375
	Validating System Designs	376
	Summary	378
	Exam Essentials	378
	Review Questions	380
Appendix A	CASP Lab Manual	385
	What You'll Need	386
	Lab A1: Download, Verify, and Install a Virtual Environment	389
	Lab A2: Explore Your Virtual Network	392
	Lab A3: Port Scanning	396

	Lab A4: Introduction to a Protocol Analyzer	400
	Lab A5: Web Vulnerabilities	406
	Lab A6: Introduction to the Nessus Vulnerability Scanner	408
	Lab A7: Verify a Baseline Security Configuration	411
	Lab A8: Basic Introduction to Windows Forensic Tools	413
	Lab A9: Introduction to Helix	421
	Lab A10: Introduction to Hashing	425
	Lab A11: File Encryption	428
	Lab A12: Cracking Encrypted Files	429
	Lab A13: Intrusion Detection	431
	Lab A14: An Introduction to Signature-Based Scanning	433
	Lab A15: Rootkit Detection	437
	Lab A16: Threat Modeling	440
	Lab A17: Introduction to the Metasploit Framework	442
	Lab A18: Social Engineering	445
	Lab A19: Routing, Switching, and Security	449
	Lab A20: Further Exploration	460
Appendix B	Answers to Review Questions	463
	Chapter 1: Cryptographic Tools and Techniques	464
	Chapter 2: Comprehensive Security Solutions	465
	Chapter 3: Securing Virtualized, Distributed, and Shared Computing	466
	Chapter 4: Host Security	467
	Chapter 5: Application Security and Penetration Testing	468
	Chapter 6: Risk Management	469
	Chapter 7: Policies, Procedures, and Incident Response	471
	Chapter 8: Security Research and Analysis	472
	Chapter 9: Enterprise Security Integration	473
	Chapter 10: Security Controls for Communication and Collaboration	474
Appendix C	About the Additional Study Tools	475
	Additional Study Tools	476
	Sybex Test Engine	476
	Electronic Flashcards	476
	PDF of Glossary of Terms	476
	Adobe Reader	476
	System Requirements	477
	Using the Study Tools	477
	Troubleshooting	477
	Customer Care	478
	<i>Index</i>	479

Table of Exercises

Exercise	2.1	Sniffing VoIP Traffic	46
Exercise	2.2	Spoofing MAC addresses with SMAC	49
Exercise	2.3	Sniffing IPv4 with Wireshark	51
Exercise	2.4	Capturing a Ping Packet with Wireshark	54
Exercise	2.5	Capturing a TCP Header with Wireshark	56
Exercise	2.6	Using Men & Mice to Verify DNS Configuration	61
Exercise	2.7	Attempting a Zone Transfer	62
Exercise	3.1	What Services Should Be Moved to the Cloud?	86
Exercise	3.2	Identifying Risks and Issues with Cloud Computing	89
Exercise	3.3	Turning to the Cloud for Large File Transfer	91
Exercise	3.4	Creating a Virtual Machine	93
Exercise	3.5	Understanding Online Storage	100
Exercise	4.1	Reviewing and Assessing ACLs	114
Exercise	4.2	Configuring IPtables	116
Exercise	4.3	Testing Your Antivirus Program	125
Exercise	4.4	Taking Control of a Router with Physical Access	130
Exercise	4.5	Running a Security Scanner to Identify Vulnerabilities	131
Exercise	4.6	Bypassing Command Shell Restrictions	132
Exercise	5.1	Identifying Testing Types at Your Organization	148
Exercise	5.2	Downloading and Running BackTrack	170
Exercise	5.3	Footprinting Your Company or Another Organization	172
Exercise	5.4	Performing TCP and UDP Port Scanning	174
Exercise	6.1	Tracking Vulnerabilities in Software	193
Exercise	6.2	Outsourcing Issues to Review	198
Exercise	6.3	Calculating Annualized Loss Expectancy	215
Exercise	7.1	Reviewing Security Policy	237
Exercise	7.2	Reviewing Documents	239
Exercise	7.3	Reviewing the Employee Termination Process	246
Exercise	7.4	Exploring Helix, a Well-Known Forensic Tool	254
Exercise	8.1	Using WinDump to Sniff Traffic	274
Exercise	8.2	Exploring the Nagios Tool	275
Exercise	8.3	Using Ophcrack	277
Exercise	8.4	Installing Firesheep	283

Exercise	8.5	Identifying XSS Vulnerabilities	284
Exercise	8.6	OpenBook	290
Exercise	9.1	Reviewing Your Company’s Acceptable Use Policy	319
Exercise	10.1	Eavesdropping on Web Conferences	346
Exercise	10.2	Sniffing Email with Wireshark.	352
Exercise	10.3	Sniffing VoIP with Cain and Abel	354

Foreword



Qualify for Jobs, Promotions, and Increased Compensation

CompTIA CASP is an international, vendor-neutral certification that helps ensure competency in:

- Enterprise security
- Risk management
- Research and analysis
- Integration of computing, communications, and business disciplines

The CASP certified individual applies critical thinking and judgment across a broad spectrum of security disciplines to propose and implement solutions that map to enterprise drivers.

It Pays to Get Certified

Certification is a great way to move ahead in your career and to gain more skills. Some ways that a certification can benefit you include:

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



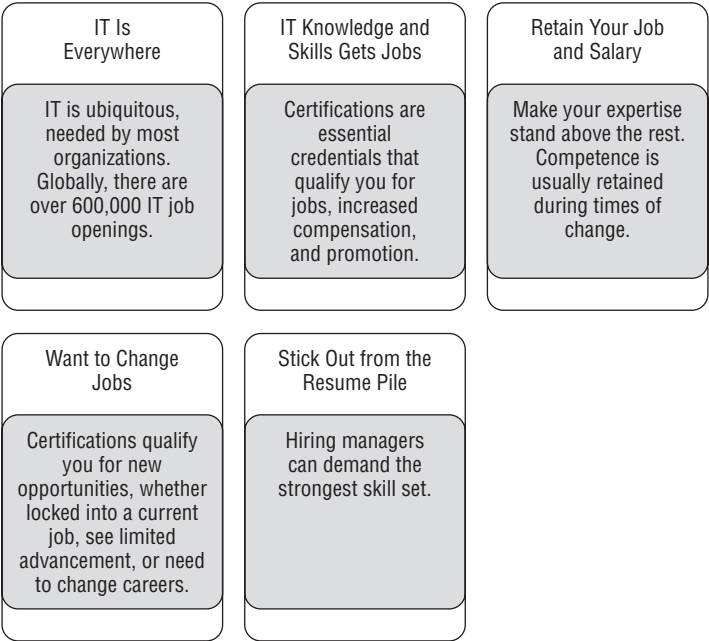
Security expertise is regularly required in organizations such as Hitachi Information Systems, Trend Micro, Lockheed Martin, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

Be the first. CASP is the first mastery level certification available from CompTIA. It expands on the widely recognized path of CompTIA Security+ with other 300,000 certified Security+ professionals.

The cloud is a new frontier. It requires astute security personnel who understand the security impact of the cloud on network design and risk.

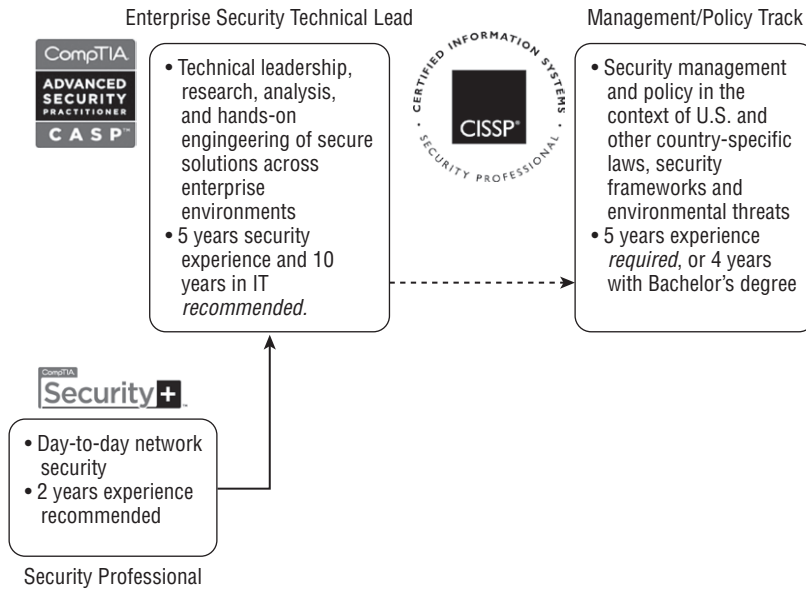
Security is one of the job categories in highest demand. And this category is growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.

How Certification Helps Your Career



CompTIA Career Pathway

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



Steps to Getting Certified

Review Exam Objectives Review the certification objectives to make sure you know what is covered in the exam. Visit <http://www.comptia.org/certifications/testprep/examobjectives.aspx>.

Practice for the Exam After you have studied for the certification, take a free assessment and sample test to get an idea what type of questions might be on the exam. Visit <http://www.comptia.org/certifications/testprep/practicetests.aspx>.

Purchase an Exam Voucher Purchase your exam voucher on the CompTIA Marketplace, which is located at www.comptiastore.com.

Take the Test! Select a certification exam provider and schedule a time to take your exam. You can find exam providers here: <http://www.comptia.org/certifications/testprep/testingcenters.aspx>.

Stay Certified! Continuing Education The 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/getCertified/certifications/casp.aspx>.

Join the IT Professional Community

The free IT Pro online community provides valuable content to students and professionals:

<http://itpro.comptia.org>

- Career IT job resources
 - Where to start in IT
 - Career assessments
 - Salary trends
 - US job search boards
- Forums on networking, security, computing, and cutting-edge technologies
- Access to blogs written by industry experts
- Current information on cutting-edge technologies
- Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This text bears the seal of CompTIA Approved Quality Content. This seal signifies this content covers 100 percent of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives. Look for this seal on other materials you use to prepare for your certification exam.



Why CompTIA?

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

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

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

Three CompTIA Certifications Ranked in the Top 10 In a 2010 study by Dice.com of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to Obtain More Information

- Visit www.comptia.org to learn more about getting a CompTIA certification. And while you're at it, take a moment to learn a little more about CompTIA, the voice of the world's IT industry. Its membership includes companies on the cutting edge of innovation.
- To contact CompTIA with any questions or comments, please call 866-835-8020, ext. 5 or email questions@comptia.org.
- Social Media. Find CompTIA on:
 - Facebook
 - LinkedIn
 - Twitter
 - YouTube



Terry Erdle
Executive Vice President, Skills Certification,
CompTIA

Introduction

The CASP certification was developed by the Computer Technology Industry Association (CompTIA) to provide an industry-wide means of certifying the competency of security professionals who have ten years' experience in IT administration and at least five years' hands-on technical experience. The security professional's job is to protect the confidentiality, integrity, and availability of an organization's valuable information assets. As such, these individuals need to have the ability to apply critical thinking and judgment.



According to CompTIA, the CASP certification “is a vendor-neutral credential.” The CASP validates “advanced-level security skills and knowledge” internationally. There is no prerequisite, but “CASP certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, ‘hands-on’ focus at the enterprise level.”

While many certification books present material for you to memorize before the exam, this book goes a step further in that it offers best practices, tips, and hands-on exercises that help those in the field of security better protect critical assets, build defense in depth, and accurately assess risk.

If you're preparing to take the CASP exam, it is a good idea to find as much information as possible about computer security practices and techniques. Because this test is designed for those with years of experience, you will be better prepared by having the most hands-on experience possible; this study guide was written with this in mind. We have included hands-on exercises, real-world scenarios, and review questions at the end of each chapter to give you some idea as to what the exam is like. You should be able to answer at least 90 percent of the test questions in this book correctly before attempting the exam; if you're unable to do so, reread the chapter and try the questions again. Your score should improve.

Before You Begin the CompTIA CASP Certification Exam

Before you begin studying for the exam, it's good for you to know that the CASP exam is offered by CompTIA (an industry association responsible for many certifications) and is granted to those who obtain a passing score on a single exam. Before you begin studying for the exam, learn all you can about the certification.



A detailed list of the CASP CAS-001 (2011 Edition) exam objectives is presented in this introduction; see the section “The CASP (2011 Edition) Exam Objectives.”

Obtaining CASP certification demonstrates that you can help your organization design and maintain system and network security services designed to secure the organization's assets. By obtaining CASP certification, you show that you have the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments.

How to Become a CASP Certified Professional

As this book goes to press candidates can take the exam at any Pearson VUE testing center. The following table contains all the necessary contact information and exam-specific details for registering. Exam pricing might vary by country or by CompTIA membership.

Vendor	Website	Phone Number
Pearson VUE	www.vue.com/comptia	U.S. and Canada: 877-551-PLUS (7587)

Who Should Read This Book?

CompTIA Advanced Security Practitioner Study Guide is designed to give you insight into the working world of IT security and describes the types of tasks and activities that a security professional with five to ten years of experience carries out. Organized classes and study groups are the ideal structures for obtaining and practicing with the recommended equipment.



College classes, training classes, and bootcamps offered by SANS and others are recommended ways to gain proficiency with the tools and techniques discussed in the book.