

TROY McMILLAN  
ROBIN ABERNATHY



# Cert Guide

Learn, prepare, and practice for exam success



CompTIA® Advanced  
Security Practitioner  
**CASP**  
CAS-002

Save 10%  
on Exam  
Voucher

See Inside

# **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

## Table of Contents

### Contents

### Introduction

### Part I: Enterprise Security

#### Chapter 1. Cryptographic Concepts and Techniques

- Cryptographic Techniques

- Cryptographic Concepts

- Cryptographic Implementations

- Review All Key Topics

#### Chapter 2. Enterprise Storage

- Storage Types

- Storage Protocols

- Secure Storage Management

- Review All Key Topics

#### Chapter 3. Network and Security Components, Concepts, and Architectures

- Advanced Network Design (Wired/Wireless)

- Security Devices

- Networking 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

# Table of Contents

Security Zones

Network Access Control

Operational and Consumer Network-Enabled Devices

Critical Infrastructure/Supervisory Control and Data Acquisition (SCADA)/ Industrial Control Systems (ICS)

Review All Key Topics

## Chapter 4. Security Controls for Hosts

Trusted OS

Endpoint Security Software

Host Hardening

Security Advantages and Disadvantages of Virtualizing Servers

Cloud-Augmented Security Services

Boot Loader Protections

Vulnerabilities Associated with Commingling of Hosts with Different Security Requirements

Virtual Desktop Infrastructure (VDI)

Terminal Services/Application Delivery Services

Trusted Platform Module (TPM)

Virtual TPM (VTPM)

Hardware Security Module (HSM)

Review All Key Topics

## Chapter 5. Application Vulnerabilities and Security Controls

Web Application Security Design Considerations

Specific Application Issues

Application Sandboxing

Application Security Frameworks

Secure Coding Standards

Software Development Methods

Database Activity Monitoring (DAM)

Web Application Firewalls (WAF)

Client-Side Processing Versus Server-Side Processing

Review All Key Topics

# **Table of Contents**

## **Part II: Risk Management and Incident Response**

### **Chapter 6. Business Influences and Associated Security Risks**

- Risk Management of New Products, New Technologies, and User Behaviors
- New or Changing Business Models/Strategies
- Security Concerns of Integrating Diverse Industries
- Ensuring That Third-Party Providers Have Requisite Levels of Information Security
- Internal and External Influences
- Impact of De-perimeterization
- Review All Key Topics

### **Chapter 7. 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 the Aggregate CIA Score
- Extreme Scenario/Worst-Case Scenario Planning
- Determine Minimum Required Security Controls Based on 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
- Review All Key Topics

### **Chapter 8. Security, Privacy Policies, and Procedures**

- 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

# **Table of Contents**

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 Various Policies

Review All Key Topics

## **Chapter 9. Incident Response and Recovery Procedures**

E-Discovery

Data Breach

Design Systems to Facilitate Incident Response

Incident and Emergency Response

Review All Key Topics

## **Part III: Research, Analysis, and Assessment**

### **Chapter 10. Industry Trends**

Perform Ongoing Research

Situational Awareness

Vulnerability Management Systems

Advanced Persistent Threats

Zero-Day Mitigating Controls and Remediation

Emergent Threats and Issues

Research Security Implications of New Business Tools

Global IA Industry/Community

Research Security Requirements for Contracts

Review All Key Topics

### **Chapter 11. Securing 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

# **Table of Contents**

- 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
- Review All Key Topics

## **Chapter 12. Assessment Tools and Methods**

- Assessment Tool Types
- Assessment Methods
- Review All Key Topics

## **Part IV: Integration of Computing, Communications, and Business Disciplines**

### **Chapter 13. Business Unit Collaboration**

- 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
- Review All Key Topics

### **Chapter 14. Secure Communication and Collaboration**

- Security of Unified Collaboration Tools
- Remote Access
- Mobile Device Management
- Over-the-Air Technologies Concerns
- Review All Key Topics

### **Chapter 15. Security Across the Technology Life Cycle**

- End-to-End Solution Ownership
- Systems Development Life Cycle (SDLC)
- Adapt Solutions to Address Emerging Threats and Security Trends 525 Asset Management (Inventory Control)

# **Table of Contents**

Asset Management (Inventory Control)

Review All Key Topics

## **Part V: Technical Integration of Enterprise Components**

### **Chapter 16. Host, Storage, Network, and Application Integration into a Secure Enterprise Architecture**

Secure Data Flows to Meet Changing Business Needs

Standards

Interoperability Issues

Technical Deployment Models

Logical and Physical Deployment Diagrams of Relevant Devices

Secure Infrastructure Design

Storage Integration (Security Considerations)

Enterprise Application Integration Enablers

Review All Key Topics

### **Chapter 17. Authentication and Authorization Technologies**

Authentication

Authorization

Attestation

Identity Propagation

Federation

Advanced Trust Models

Review All Key Topics

## **Part VI: Appendixes**

Appendix A: Answers

Appendix B: CASP CAS-002 Exam Updates

Always Get the Latest at the Companion Website

Glossary

Index

CD-only Elements:



# **Table of Contents**

Appendix C: Memory Tables

Appendix D: Memory Tables Answer Key