Certified Information Systems Security Professional (CISSP)

Summary

Length: 20 hours Level: Experienced

Start your prep for the ISC2 Certified Information Systems Security Professional certification with the uCertify course and labs. Lab simulates real-world, hardware, software, and command-line interface environments and can be mapped to any textbook, course, or training. The Information Systems Security certification course and lab cover exam objectives thoroughly and teach the principles of effective system security. Lessons and TestPrep will further prepare candidates for this certification exam with interactive item types.

Learning Objectives

The ISC2 CISSP certification is a highly acknowledged cybersecurity credential. This certification is ideal for professionals who are looking to demonstrate their knowledge across different security practices and principles. By earning this credential you will be able to implement, design, and effectively manage a cybersecurity program. This certification provides information security professionals with an objective to measure competence and a globally recognized standard of achievement

Course Outline

1. Introduction

   Overview of the CISSP Exam
   The Elements of This Study Guide
   Interactive Online Learning Environment and TestBank
   Study Guide Exam Objectives
   Objective Map

2. Security Governance Through Principles and Policies

   Security 101
   Understand and Apply Security Concepts
   Security Boundaries
   Evaluate and Apply Security Governance Principles
   Manage the Security Function
   Security Policy, Standards, Procedures, and Guidelines
   Threat Modeling
   Supply Chain Risk Management
   Summary
   Exam Essentials
   Written Lab

3. Personnel Security and Risk Management Concepts

   Personnel Security Policies and Procedures
   Understand and Apply Risk Management Concepts
   Social Engineering
   Establish and Maintain a Security Awareness, Education, and Training Program
   Summary
   Exam Essentials
   Written Lab

4. Business Continuity Planning

Planning for Business Continuity
Project Scope and Planning
Business Impact Analysis
Continuity Planning
Plan Approval and Implementation
Summary
Exam Essentials
Written Lab

5. Laws, Regulations, and Compliance

Categories of Laws
Laws
State Privacy Laws
Compliance
Contracting and Procurement
Summary
Exam Essentials
Written Lab

6. Protecting Security of Assets

Identifying and Classifying Information and Assets
Establishing Information and Asset Handling Requirements
Data Protection Methods
Understanding Data Roles
Using Security Baselines
Summary
Exam Essentials
Written Lab

7. Cryptography and Symmetric Key Algorithms

Cryptographic Foundations
Modern Cryptography
Symmetric Cryptography
Cryptographic Lifecycle
Summary
Exam Essentials
Written Lab

8. PKI and Cryptographic Applications

Asymmetric Cryptography
Hash Functions
Digital Signatures
Public Key Infrastructure
Asymmetric Key Management
Hybrid Cryptography
Applied Cryptography
Cryptographic Attacks
Summary
Exam Essentials
Written Lab

9. Principles of Security Models, Design, and Capabilities

Secure Design Principles
Techniques for Ensuring CIA
Understand the Fundamental Concepts of Security Models
Select Controls Based on Systems Security Requirements

Understand Security Capabilities of Information Systems
Summary
Exam Essentials
Written Lab

10. Security Vulnerabilities, Threats, and Countermeasures

Shared Responsibility
"Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements"
Client-Based Systems
Server-Based Systems
Industrial Control Systems
Distributed Systems
High-Performance Computing (HPC) Systems
Internet of Things
Edge and Fog Computing
Embedded Devices and Cyber-Physical Systems
Specialized Devices
Microservices
Infrastructure as Code
Virtualized Systems
Containerization
Serverless Architecture
Mobile Devices
Essential Security Protection Mechanisms
Common Security Architecture Flaws and Issues
Summary
Exam Essentials
Written Lab

11. Physical Security Requirements

Apply Security Principles to Site and Facility Design
Implement Site and Facility Security Controls
Implement and Manage Physical Security
Summary
Exam Essentials
Written Lab

12. Secure Network Architecture and Components

OSI Model
TCP/IP Model
Analyzing Network Traffic
Common Application Layer Protocols
Transport Layer Protocols
Domain Name System
Internet Protocol (IP) Networking
ARP Concerns
Secure Communication Protocols
Implications of Multilayer Protocols
Microsegmentation
Wireless Networks
Other Communication Protocols
Cellular Networks
Content Distribution Networks (CDNs)
Secure Network Components
Summary
Exam Essentials
Written Lab

13. Chapter 13: Secure Communications and Network Attacks

Protocol Security Mechanisms
Secure Voice Communications
Remote Access Security Management
Multimedia Collaboration
Load Balancing
Manage Email Security
Virtual Private Network
Switching and Virtual LANs
Network Address Translation
Third-Party Connectivity
Switching Technologies
WAN Technologies
Fiber-Optic Links
Security Control Characteristics
Prevent or Mitigate Network Attacks
Summary
Exam Essentials
Written Lab

14. Managing Identity and Authentication

Controlling Access to Assets
Managing Identification and Authentication
Implementing Identity Management
Managing the Identity and Access Provisioning Lifecycle
Summary
Exam Essentials
Written Lab

15. Controlling and Monitoring Access

Comparing Access Control Models
Implementing Authentication Systems
Understanding Access Control Attacks
Summary
Exam Essentials
Written Lab

16. Security Assessment and Testing

Building a Security Assessment and Testing Program
Performing Vulnerability Assessments
Testing Your Software
Implementing Security Management Processes
Summary
Exam Essentials
Written Lab

17. Managing Security Operations

Apply Foundational Security Operations Concepts
Addressing Personnel Safety and Security
Provision Resources Securely
Apply Resource Protection
Managed Services in the Cloud
Perform Configuration Management (CM)
Managing Change
Managing Patches and Reducing Vulnerabilities
Summary

Exam Essentials
Written Lab

18. Preventing and Responding to Incidents

Conducting Incident Management
Implementing Detective and Preventive Measures
Logging and Monitoring
Automating Incident Response
Summary
Exam Essentials
Written Lab

19. Disaster Recovery Planning

The Nature of Disaster
Understand System Resilience, High Availability, and Fault Tolerance
Recovery Strategy
Recovery Plan Development
Training, Awareness, and Documentation
Testing and Maintenance
Summary
Exam Essentials
Written Lab

20. Investigations and Ethics

Investigations
Major Categories of Computer Crime
Ethics
Summary
Exam Essentials
Written Lab

21. Software Development Security

Introducing Systems Development Controls
Establishing Databases and Data Warehousing
Storage Threats
Understanding Knowledge-Based Systems
Summary
Exam Essentials
Written Lab

22. Malicious Code and Application Attacks

Malware
Malware Prevention
Application Attacks
Injection Vulnerabilities
Exploiting Authorization Vulnerabilities
Exploiting Web Application Vulnerabilities
Application Security Controls
Secure Coding Practices
Summary
Exam Essentials
Written Lab

Audience

This course is intended for experienced IT security-related practitioners, auditors, consultants, investigators, or instructors, including network or security analysts and engineers, network administrators, information security specialists, and risk management professionals, who are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current computer security careers or to migrate to a related career.

Prerequisites

While there are no prerequisites for this course, please ensure you have the right level of experience to be successful in this training.