uCertify

Course Outline

Certified Information Systems Security Professional (CISSP)



28 Mar 2024

1. Course Objective
2. Pre-Assessment
3. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
4. Expert Instructor-Led Training
5. ADA Compliant & JAWS Compatible Platform
6. State of the Art Educator Tools
7. Award Winning Learning Platform (LMS)
8. Chapter & Lessons

   Syllabus

   Chapter 1: Introduction

   Chapter 2: Security Governance Through Principles and Policies

   Chapter 3: Personnel Security and Risk Management Concepts

   Chapter 4: Business Continuity Planning

   Chapter 5: Laws, Regulations, and Compliance

   Chapter 6: Protecting Security of Assets

   Chapter 7: Cryptography and Symmetric Key Algorithms

   Chapter 8: PKI and Cryptographic Applications

   Chapter 9: Principles of Security Models, Design, and Capabilities

   Chapter 10: Security Vulnerabilities, Threats, and Countermeasures

   Chapter 11: Physical Security Requirements

   Chapter 12: Secure Network Architecture and Components

   Chapter 13: Secure Communications and Network Attacks

   Chapter 14: Managing Identity and Authentication

   Chapter 15: Controlling and Monitoring Access

   Chapter 16: Security Assessment and Testing

   Chapter 17: Managing Security Operations

   Chapter 18: Preventing and Responding to Incidents

Chapter 19: Disaster Recovery Planning

Chapter 20: Investigations and Ethics

Chapter 21: Software Development Security

Chapter 22: Malicious Code and Application Attacks

Videos and How To

9. Practice Test

   Here's what you get

   Features

10. Live labs

    Lab Tasks

    Here's what you get

11. Post-Assessment

1. Course Objective

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.

2. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. Quizzes

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.



4. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.



5. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.



6. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

7. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

8. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

9. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution

2. Best Virtual Learning Solution
3. Best Student Assessment Solution
4. Best Postsecondary Learning Solution
5. Best Career and Workforce Readiness Solution
6. Best Instructional Solution in Other Curriculum Areas
7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform
    2. Best Instructional Solution in Other Curriculum Areas
    3. Best Learning Relationship Management Solution

- **2019**
    1. Best Virtual Learning Solution
    2. Best Content Authoring Development or Curation Solution
    3. Best Higher Education Learning Management Solution (LMS)

- **2020**

1. Best College and Career Readiness Solution
2. Best Cross-Curricular Solution
3. Best Virtual Learning Solution

10. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Introduction

- Overview of the CISSP Exam
- The Elements of This Study Guide
- Study Guide Exam Objectives
- Objective Map

Chapter 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

Chapter 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

Chapter 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

Chapter 5: Laws, Regulations, and Compliance

- Categories of Laws
- Laws
- State Privacy Laws
- Compliance
- Contracting and Procurement
- Summary

- Exam Essentials
- Written Lab

Chapter 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

Chapter 7: Cryptography and Symmetric Key Algorithms

- Cryptographic Foundations
- Modern Cryptography
- Symmetric Cryptography
- Cryptographic Lifecycle
- Summary

- Exam Essentials
- Written Lab

Chapter 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

Chapter 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

Chapter 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

Chapter 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

Chapter 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

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

Chapter 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

Chapter 15: Controlling and Monitoring Access

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

Chapter 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

Chapter 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

Chapter 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

Chapter 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

Chapter 20: Investigations and Ethics

- Investigations
- Major Categories of Computer Crime
- Ethics
- Summary
- Exam Essentials

- Written Lab

Chapter 21: Software Development Security

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

Chapter 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

11. Practice Test

Here's what you get

108	3	108
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode, learners can read through one item at a time without attempting it.

12. Live Labs

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

Lab Tasks

Security Governance Through Principles and Policies

- Encrypting the Disk
- Encrypting a File or Folder
- Understanding documentation review

Personnel Security and Risk Management Concepts

- Understanding and Applying Risk Management Concepts
- Understanding Security Controls

Business Continuity Planning

- Understanding Business Continuity Planning

Laws, Regulations, and Compliance

- Understanding Laws related to IT

Protecting Security of Assets

- Understanding Data Loss Prevention System

Cryptography and Symmetric Key Algorithms

- Understanding Cryptographic Systems
- Understanding Symmetric Encryption Algorithms

PKI and Cryptographic Applications

- Observing an MD5-Generated Hash Value
- Observing an SHA-Generated Hash Value
- Using OpenSSL to Create a Public/Private Key Pair
- Understanding the Diffie-Hellman Algorithm
- Understanding the RSA Algorithm
- Hiding Text Using Steganography
- Understanding the Hardware Security Module

Principles of Security Models, Design, and Capabilities

- Understanding Secure Design Principles
- Understanding Evaluation Assurance Levels
- Understanding Constrained Interface

Security Vulnerabilities, Threats, and Countermeasures

- Understanding the Lifecycle of an Executed Process
- Understanding the Internet Files Cache
- Understanding Hypervisor
- Understanding a Rootkit

Physical Security Requirements

- Understanding Fire Detection Systems
- Understanding Security Controls
- Understanding Programmable Lock

Secure Network Architecture and Components

- Understanding the OSI Model
- Understanding the Application Layer Protocols
- Configuring IPSec
- Understanding IP Classes
- Understanding Virtual eXtensible LAN
- Understanding 802.11 Wireless Networking Amendments
- Understanding LiFi and Zigbee
- Using Windows Firewall
- Understanding Network Topologies

Secure Communications and Network Attacks

- Configuring a VPN
- Understanding IPsec's Encryption of a Packet in Transport and Tunnel Modes
- Configuring VLANs
- Configuring Dynamic NAT
- Configuring Static NAT
- Understanding NAT and PAT
- Understanding Third-Party Connectivity
- Understanding Circuit Switching and Packet Switching

Managing Identity and Authentication

- Restricting Local Accounts

Controlling and Monitoring Access

- Assigning Permissions to Folders

- Examining Kerberos Settings
- Performing Spoofing
- Simulating an Eavesdropping Attack Using Wireshark
- Using Rainbow Tables

Security Assessment and Testing

- Configuring Audit Group Policy
- Using nmap for Scanning
- Conducting Vulnerability Scanning Using Nessus
- Exploiting Windows 7 Using Metasploit
- Scanning Ports Using Metasploit
- Understanding Penetration Testing
- Understanding Penetration Tests
- Understanding the Fagan Inspections
- Understanding Training and Awareness Program

Managing Security Operations

- Understanding Security Operations
- Understanding Privileged Account Management
- Understanding Cloud Shared Responsibility Model

Preventing and Responding to Incidents

- Performing DoS Attack with SYN Flood
- Enabling Intrusion Prevention and Detection
- Understanding Honeypots and Honeynets
- Understanding Security Information and Event Management

Disaster Recovery Planning

- Configuring RAID 5
- Taking Incremental Backup
- Taking a Full Backup

Investigations and Ethics

- Completing the Chain of Custody
- Understanding Organizational Code of Ethics

Software Development Security

- Understanding Software Development Lifecycle
- Understanding Software Capability Maturity Model
- Understanding ACID Model
- Understanding a Neural Network

Malicious Code and Application Attacks

- Causing a DarkComet Trojan Infection
- Understanding Antimalware Software
- Exploiting a Website Using SQL Injection
- Conducting a Cross-Site Request Forgery Attack
- Attacking a Website Using XSS Injection

Here's what you get

80	33	01:05
LIVE LABS	VIDEO TUTORIALS	HOURS

13. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com