uCertify

Course Outline

ISC2 CISSP Study Guide 8th edition

Lesson Practice test Lab

30 Jul 2020

Contents

1. Course Objective

Prepare for the ISC2 CISSP certification exam with the CISSP course and lab. The lab is versatile and delivers a hands-on experience, replacing expensive physical labs. The course and labs offer an interactive learning experience in areas such as security and risk management, asset security, security architecture, and engineering, identity and access management (IAM), security assessment and testing, security operations, and software development security.

2. Pre-Assessment

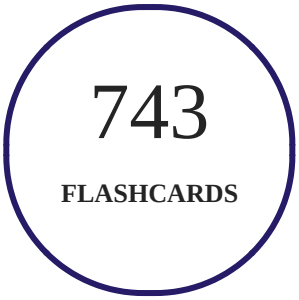
Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

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 assignments. 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
- Notes on This Course's Organization

Chapter 2: Security Governance Through Principles and Policies

- Understand and Apply Concepts of Confidentiality, Integrity, and Availability
- Evaluate and Apply Security Governance Principles
- Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines
- Understand and Apply Threat Modeling Concepts and Methodologies
- Apply Risk-Based Management Concepts to the Supply Chain
- Summary
- Exam Essentials
- Written Lab

Chapter 3: Personnel Security and Risk Management Concepts

- Personnel Security Policies and Procedures
- Security Governance
- Understand and Apply Risk Management Concepts
- Establish and Maintain a Security Awareness, Education, and Training Program
- Manage the Security Function
- Summary

- Exam Essentials
- Written Lab

Chapter 4: Business Continuity Planning

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

Chapter 5: Laws, Regulations, and Compliance

- Categories of Laws
- Laws
- Compliance
- Contracting and Procurement

- Summary
- Exam Essentials
- Written Lab

Chapter 6: Protecting Security of Assets

- Identify and Classify Assets
- Determining Ownership
- Using Security Baselines
- Summary
- Exam Essentials
- Written Lab

Chapter 7: Cryptography and Symmetric Key Algorithms

- Historical Milestones in Cryptography
- Cryptographic Basics
- 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
- Applied Cryptography
- Cryptographic Attacks
- Summary
- Exam Essentials
- Written Lab

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

- Implement and Manage Engineering Processes Using Secure Design Principles

- 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

- Assess and Mitigate Security Vulnerabilities
- Client-Based Systems
- Server-Based Systems
- Database Systems Security
- Distributed Systems and Endpoint Security
- Internet of Things
- Industrial Control Systems
- Assess and Mitigate Vulnerabilities in Web-Based Systems
- Assess and Mitigate Vulnerabilities in Mobile Systems
- Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems

- Essential Security Protection Mechanisms
- Common Architecture Flaws and Security 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 Securing Network Components

- OSI Model
- TCP/IP Model
- Converged Protocols

- Wireless Networks
- Secure Network Components
- Cabling, Wireless, Topology, Communications, and Transmission Media Technology
- Summary
- Exam Essentials
- Written Lab

Chapter 13: Secure Communications and Network Attacks

- Network and Protocol Security Mechanisms
- Secure Voice Communications
- Multimedia Collaboration
- Manage Email Security
- Remote Access Security Management
- Virtual Private Network
- Virtualization
- Network Address Translation
- Switching Technologies

- WAN Technologies
- Miscellaneous Security Control Characteristics
- Security Boundaries
- Prevent or Mitigate Network Attacks
- Summary
- Exam Essentials
- Written Lab

Chapter 14: Managing Identity and Authentication

- Controlling Access to Assets
- Comparing 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
- 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

- Applying Security Operations Concepts
- Securely Provisioning Resources

- Managing Configuration
- Managing Change
- Managing Patches and Reducing Vulnerabilities
- Summary
- Exam Essentials
- Written Lab

Chapter 18: Preventing and Responding to Incidents

- Managing Incident Response
- Implementing Detective and Preventive Measures
- Logging, Monitoring, and Auditing
- Summary
- Exam Essentials
- Written Lab

Chapter 19: Disaster Recovery Planning

- The Nature of Disaster
- Understand System Resilience 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
- Storing Data and Information
- Understanding Knowledge-Based Systems
- Summary
- Exam Essentials
- Written Lab

Chapter 22: Malicious Code and Application Attacks

- Malicious Code
- Password Attacks
- Application Attacks
- Web Application Security
- Reconnaissance Attacks
- Masquerading Attacks
- Summary
- Exam Essentials
- Written Lab

11. Practice Test

uCertify provides full length practice tests. These tests closely follow the exam objectives and are designed to simulate real exam conditions. Each course has a number of test sets consisting of hundreds of items to ensure that learners are prepared for the certification exam.

Here's what you get

116
PRE-ASSESSMENTS QUESTIONS

115
POST-ASSESSMENTS QUESTIONS

Features

Full Remediation

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.

Learn, Test and Review Mode

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. Performance Based Labs

uCertify's performance-based labs are Live Labs. Learn the real world skills using Live Labs. uCertify Labs are cloud-based, device-enabled and can be easily integrated with an LMS. Features of uCertify labs:

- Provide hands-on experience in a safe, online environment
- Labs simulate real world, hardware, software & CLI environment
- Flexible and inexpensive alternative to physical Labs
- Comes with well-organized component library for every task
- Highly interactive - learn by doing
- Explanations and remediation available
- Videos on how to perform

Lab Tasks

- Encrypting the Disk
- Encrypting a File or Folder
- Configuring Audit Group Policy
- Completing the Chain of Custody
- Assigning Permissions to Folders
- Identifying risk actions
- Understanding elements of risk
- Identifying steps in quantitative risk analysis
- Configuring Standard Access Control List

- Configuring Extended Access Control List
- Identifying phases in BCP process
- Identifying CFAA provisions
- Checking the integrity of messages through MAC values
- Identifying asymmetric algorithms
- Identifying cryptographic attacks
- Using OpenSSL to Create a Public/Private Key Pair
- Observe an SHA-Generated Hash Value
- Observing an MD5-Generated Hash Value
- Identifying sequence of sender's process in digital signature system
- Understanding PKCS standards
- Identifying Information models
- Identifying protection mechanisms
- Identifying OSI layer functions
- Identifying OSI layers
- Identifying steps in the encapsulation/decapsulation process
- Identifying connectionless communication
- Identifying abbreviations for various Internet layer protocols
- Identifying TCP/IP protocol layers
- Identifying TCP/IP layers
- Identifying flag bit designator
- Using Windows Firewall
- Configuring Linux Firewall Using Iptable
- Identifying gateway firewalls
- Identifying hardware devices
- Connecting systems to the Internet through a router
- Identifying firewall techniques
- Identifying types of cable
- Identifying components of a coaxial cable
- Identifying network topologies
- Identifying UTP categories
- Identifying steps in CSMA technology
- Identifying LAN sub technologies

- Configuring IPSec
- Configuring VLAN
- Identifying secure communication protocols
- Identifying authentication protocols
- Identifying phreaker tools
- Identifying security solutions
- Configuring a VPN
- Identifying VPN protocols
- Configuring Static NAT
- Configuring Dynamic NAT
- Understanding NAT
- Identifying switching technology properties
- Identifying specialized protocols
- Understanding transparency
- Understanding security boundaries
- Using Ettercap for ARP Spoofing
- Identifying types of Denial of Service attacks
- Identifying access control types
- Identifying authorization mechanisms
- Restricting Local Accounts
- Identifying drawbacks of Kerberos authentication
- Identifying components of the Kerberos authentication protocol
- Identifying authentication services
- Identifying responsibilities
- Reviewing an Authorization Letter for Penetration Testing
- Identifying attacks
- Identifying social engineering attacks
- Configuring User Access Control Setting
- Scanning Ports Using Metasploit
- Exploiting Windows 7 Using Metasploit
- Enabling a Keylogger in a Target Machine
- Conducting Vulnerability Scanning Using Nessus
- Using nmap for Scanning

- Identifying terms associated with data destruction
- Identifying steps within an effective patch management program
- Identifying steps in incident response management
- Enabling Intrusion Prevention and Detection
- Configuring Snort
- Identifying malicious attacks
- Working with a host-based IDS
- Identifying sequence in which the IDS instructs the TCP to reset connections
- Performing DoS Attack with SYN Flood
- Identifying RAID level characteristics
- Identifying processing sites in disaster recovery plan
- Identifying disaster recovery plan tests
- Taking a Full Backup
- Taking Incremental Backup
- Configuring RAID 5
- Identifying computer crime types
- Identifying stages in a waterfall lifecycle model
- Understanding object-oriented programming terms
- Identifying levels in Software Capability Maturity Model
- Identifying testing methods
- Identifying primary phases of SDLC
- Identifying keys in a database
- Identifying storage types
- Causing a DarkComet Trojan Infection
- Identifying types of viruses
- Identifying types of viruses
- Using the John the Ripper Tool
- Using Social Engineering Techniques to Plan an Attack
- Attacking a Website Using XSS Injection
- Conducting a Cross-Site Request Forgery Attack
- Exploiting a Website Using SQL Injection
- Understanding application attacks
- Defending against IP Spoofing
- Using Burp Suite

Here's what you get

109

PERFORMANCE BASED LAB

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.

CONNECT WITH US

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.uCertify.com