Course Ou

CISSP - Certified Information Systems
2015 (Course & Lab



28 Mar 2024

Contents

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: Access Control

   Chapter 2: Access Control Attacks and Monitoring

   Chapter 3: Secure Network Architecture and Securing Network Components

   Chapter 4: Secure Communications and Network Attacks

   Chapter 5: Security Governance Concepts, Principles, and Policies

   Chapter 6: Risk and Personnel Management

   Chapter 7: Software Development Security

   Chapter 8: Malicious Code and Application Attacks

   Chapter 9: Cryptography and Symmetric Key Algorithms

   Chapter 10: PKI and Cryptographic Applications

   Chapter 11: Principles of Security Models, Design, and Capabilities

   Chapter 12: Security Architecture Vulnerabilities, Threats, and Countermeasures

   Chapter 13: Security Operations

   Chapter 14: Incident Management

   Chapter 15: Business Continuity Planning

Chapter 16: Disaster Recovery Planning

Chapter 17: Laws, Regulations, and Compliance

Chapter 18: Incidents and Ethics

Chapter 19: Physical Security Requirements

Chapter 20: Appendix A

Videos and How To

9. Practice Test

   Here's what you get

   Features

10. Performance Based labs

    Lab Tasks

    Here's what you get

11. Post-Assessment

1. Course Objective

Gain hands-on expertise in CISSP certification exam by CISSP-2015 course and performance based labs. Performance based labs simulate real-world, hardware, software & command line interface environments and can be mapped to any text-book, course & training. CISSP certification is vendor-neutral credential designed for IT security practitioners to validate their technical and managerial skills, credibility and, experience. CISSP exam is designed to engineer, implement, and manage the overall information security program to protect organizations from growing sophisticated attacks.

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.

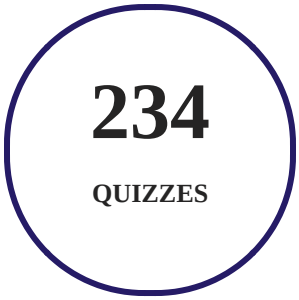
3. Exercises

There is no limit to the number of times learners can attempt these. Exercises come with detailed remediation, which ensures that learners are confident on the topic before proceeding.



4. 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.



5. 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.



6. 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.



7. 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.

8. 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.

9. 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.

10. 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

11. 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: Access Control

- Access Control Overview
- Identification and Authentication Techniques
- Access Control Techniques

- Authorization Mechanisms
- Identity and Access Provisioning Life Cycle
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 2: Access Control Attacks and Monitoring

- Understanding Access Control Attacks
- Preventing Access Control Attacks
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 3: Secure Network Architecture and Securing Network Components

- OSI Model
- Secure Network Components
- Cabling, Wireless, Topology, and Communications Technology
- Summary

- Exam Essentials
- Review All the Key Topics

Chapter 4: Secure Communications and Network Attacks

- Network and Protocol Security Mechanisms
- Virtual Private Network
- Remote Access Security Management
- Network Address Translation
- Switching Technologies
- WAN Technologies
- Virtualization
- Miscellaneous Security Control Characteristics
- Manage Email Security
- Secure Voice Communications
- Security Boundaries
- Network Attacks and Countermeasures
- Summary
- Exam Essentials

- Review All the Key Topics

Chapter 5: Security Governance Concepts, Principles, and Policies

- Security Management Planning
- Security Governance
- Security Roles and Responsibilities
- Protection Mechanisms
- Privacy Requirements Compliance
- Control Frameworks: Planning to Plan
- Security Management Concepts and Principles
- Develop and Implement Security Policy
- Change Control/Management
- Data Classification
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 6: Risk and Personnel Management

- Manage Third-Party Governance

- Risk Management
- Manage Personnel Security
- Develop and Manage Security Education, Training, and Awareness
- Manage the Security Function
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 7: Software Development Security

- Application Issues
- Databases and Data Warehousing
- Data/Information Storage
- Knowledge-Based Systems
- Systems Development Controls
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 8: Malicious Code and Application Attacks

- Malicious Code
- Password Attacks
- Application Attacks
- Web Application Security
- Reconnaissance Attacks
- Masquerading Attacks
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 9: Cryptography and Symmetric Key Algorithms

- Historical Milestones in Cryptography
- Cryptographic Basics
- Modern Cryptography
- Symmetric Cryptography
- Cryptographic Life Cycle
- Summary
- Exam Essentials

- Review All the Key Topics

Chapter 10: PKI and Cryptographic Applications

- Asymmetric Cryptography
- Hash Functions
- Digital Signatures
- Public Key Infrastructure
- Asymmetric Key Management
- Applied Cryptography
- Cryptographic Attacks
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 11: Principles of Security Models, Design, and Capabilities

- Understand the Fundamental Concepts of Security Models
- Objects and Subjects
- Understand the Components of Information Systems Security Evaluation Models

- Understand Security Capabilities Of Information Systems
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 12: Security Architecture Vulnerabilities, Threats, and Countermeasures

- Computer Architecture
- Avoiding Single Points of Failure
- Distributed Architecture
- Security Protection Mechanisms
- Common Flaws and Security Issues
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 13: Security Operations

- Security Operations Concepts
- Resource Protection
- Patch and Vulnerability Management

- Change and Configuration Management
- Security Audits and Reviews
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 14: Incident Management

- Managing Incident Response
- Implement Preventive Measures Against Attacks
- Understand System Resilience and Fault Tolerance
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 15: Business Continuity Planning

- Planning for Business Continuity
- Project Scope and Planning
- Business Impact Assessment

- Continuity Planning
- BCP Documentation
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 16: Disaster Recovery Planning

- The Nature of Disaster
- Recovery Strategy
- Recovery Plan Development
- Training and Documentation
- Testing and Maintenance
- Categories of Laws
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 17: Laws, Regulations, and Compliance

- Laws

- Compliance
- Contracting and Procurement
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 18: Incidents and Ethics

- Investigations
- Major Categories of Computer Crime
- Incident Handling
- Ethics
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 19: Physical Security Requirements

- Site and Facility Design Considerations
- Forms of Physical Access Controls

- Technical Controls
- Environment and Life Safety
- Equipment Failure
- Privacy Responsibilities and Legal Requirements
- Summary
- Exam Essentials
- Review All the Key Topics

Chapter 20: Appendix A

12.  Practice Test

Here's what you get

109	3	100
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.

13.  Performance Based Labs

uCertify's performance-based labs are simulators that provides virtual environment. Labs deliver hands on experience with minimal risk and thus replace expensive physical 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

- Identifying access control types
- Disabling a service
- Identifying drawbacks of Kerberos authentication
- Identifying components of the Kerberos authentication protocol
- Identifying authentication services

- Creating a password for account
- Configuring password policies
- Enabling and disabling password expiration
- Configuring NPS to provide RADIUS authentication
- Configuring NPS network policy
- Configuring the server
- Creating and configuring a network
- Identifying authorization mechanisms
- Identifying responsibilities
- Identifying types of system attack
- Identifying attacks
- Identifying social engineering attacks
- Filtering entries in Event Viewer
- Viewing password hashes
- Configuring audit policies
- Viewing different event details
- Identifying log types
- Identifying OSI layer functions
- Identifying OSI layers
- Identifying connectionless communication
- Identifying abbreviations for various Internet layer protocols
- Identifying TCP/IP protocol layers
- Identifying TCP/IP layers
- Configuring IPv4 address
- Identifying application layer protocols
- Identifying steps in the encapsulation/decapsulation process
- Identifying flag bit designator
- Identifying gateway firewalls
- Identifying hardware devices
- Connecting Systems to the Internet Through a Firewall Router
- Identifying firewall techniques
- Identifying types of cable
- Identifying components of a coaxial cable
- Configuring Windows 7 wireless settings
- Configuring SSID

- Identifying network topologies
- Identifying UTP categories
- Identifying steps in CSMA technology
- Identifying LAN sub technologies
- Identifying secure communication protocols
- Identifying authentication protocols
- Creating a remote access VPN connection
- Identifying VPN protocols
- Connecting to a server using Remote Desktop Connection
- Creating a dial-up connection
- Understanding NAT
- Identifying switching technology properties
- Installing Windows Virtual PC
- Identifying specialized protocols
- Creating a virtual PC machine
- Understanding transparency
- Identifying security solutions
- Identifying phreaker tools
- Understanding security boundaries
- Identifying types of Denial of Service attacks
- Identifying security management plans
- Identifying protection mechanisms
- Identifying steps in a classification scheme
- Identifying risk actions
- Understanding elements of risk
- Identifying steps in quantitative risk analysis
- Identifying types of malware
- Understanding agents
- Identifying keys in a database
- Identifying storage types
- Identifying stages in a waterfall lifecycle model
- Identifying generations of languages
- Understanding object-oriented programming terms
- Identifying levels in Software Capability Maturity Model
- Identifying testing methods

- Identifying primary phases of SDLC
- Identifying types of viruses
- Understanding application attacks
- Identifying types of viruses
- Installing the AVG antivirus and scanning a drive
- Checking the integrity of messages through MAC values
- Identifying asymmetric algorithms
- Identifying cryptographic attacks
- Identifying sequence of sender's process in digital signature system
- Backing up an encryption certificate and key
- Understanding PKCS standards
- Identifying Information models
- Identifying TCSEC categories
- Identifying computer activities
- Disabling the COM and parallel ports
- Installing SDRAM and DDR memory modules
- Connecting speakers to a computer
- Connecting a keyboard, mouse, and monitor to a computer
- Understanding process scheduler
- Identifying RAID levels
- Identifying service associated with cloud computing
- Identifying terms associated with data destruction
- Identifying steps within an effective patch management program
- Identifying security reviews
- Identifying steps in incident response management
- Identifying sequence in which the IDS instructs the TCP to reset connections
- Working with a host-based IDS
- Identifying malicious attacks
- Identifying RAID level characteristics
- Identifying phases in BCP process
- Identifying man-made threats
- Identifying processing sites in disaster recovery plan
- Identifying disaster recovery plan tests
- Identifying CFAA provisions
- Identifying computer crime types

- Identifying physical access control mechanisms
- Identifying terms associated with power issues
- Identifying primary stages of fire

Here's what you get

113	27	33
PERFORMANCE BASED LAB	VIDEO TUTORIALS	MINUTES

14. 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