
CYBRARY

Course Syllabus

CISSP

Instructor Name: Kelly Handerhan

Instructor Website: CyberTrain.it

Instructor Contact: KellyH@CyberTrain.IT

Course Creation Date: 6/13/2019

Course Description and Goals

Course Description: The CISSP certification from ISC2 is one of the premier certifications in the Information Security industry. Covering numerous topics across 8 Domains, this certification speaks to a well-rounded understanding of the many facets of protecting organizational assets. Designed around eight specific domains, this course examines : Security & Risk Management , Asset Security, Security Architecture and Engineering, Communication & Network Security, Identity & Access management , Security Assessment & Testing, Security Operations and Software Development Security.

Prerequisites: To earn this certification, you must pass the exam as well as have 5 years of paid experience in two or more domains of the CISSP Common Body of Knowledge. However, if you have passed the examination but are short of the requisite experience, you can become an Associate of (ISC)². Thereafter, you will have 6 years' to earn the requisite experience.

Study Resources: All supplemental materials will be provided in the 'resources' tab of the course page!

Course Goals: By the end of this course, students should be able to:

- ☐ Pass the CISSP Exam

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

Labs and Assessments Used:

This course will use labs and assessments from the Cybrary lab environment. All labs and assessments must be completed to attain Cybrary's Certification of Completion, but may not be necessary for your exam preparation process depending on your prior experience. The items are shown below in the order they appear, each lab will appear in the same module as its relevant CISSP topic. If you are having trouble completing the CISSP Labs, try to launch the lab, then return to the Lecture/Lab Guidance in the previous lesson and complete the lab while viewing the instructor.

- Creation of BCP and DRP (CYBRScore)
- ISC2 CISSP Practice Test: Certified Information Systems Security Professional (Kaplan Practice Test)

Course Outline

Module 1 | Welcome and Introduction

Lesson 1.1: Introduction (08:22)

Lesson 1.2: Computer Adaptive Testing (CAT) (4:31)

Module 2 | Information Security and Risk Management

Lesson 2.1: Domain 1 Agenda (04:19)

Lesson 2.2: Information Security Program Part 1 (11:30)

Lesson 2.3: Information Security Program Part 2 (08:16)

Lesson 2.4: Roles and Responsibilities (12:58)

Lesson 2.5: Risk Definitions (07:35)

Lesson 2.6: Risk Identification (09:14)

Lesson 2.7: Risk Assessment and Analysis (14:58)

Lesson 2.8: Risk Mitigation and Response (10:21)

Lesson 2.9: Risk Monitoring and Reporting (08:14)

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

- Lesson 2.10: Legal Considerations (09:24)
- Lesson 2.11: Knowledge Transfer (05:39)
- Lesson 2.12: The CISSP Mindset Part 1 (09:16)
- Lesson 2.13: The CISSP Mindset Part 2 (11:40)
- Lesson 2.15: Introduction to Business Continuity and Disaster Recovery Planning (04:08)
- Lesson 2.16: Business Continuity Planning Part 1 (09:28)
- Lesson 2.17: Business Continuity Planning Part 2 (07:32)
- Lesson 2.18: BCP Step 1: Project Scope and Planning Part 1 (05:06)
- Lesson 2.19: BCP Step 1: Project Scope and Planning Part 2 (05:04)
- Lesson 2.20: BCP Step 2: Business Impact Assessment Part 1 (06:44)
- Lesson 2.21: BCP Step 2: Business Impact Assessment Part 2 (07:15)
- Lesson 2.22: BCP Steps 3 and 4: Community Planning, Approval and Implementation (10:58)
- Lesson 2.23: BCP Sub Plans 07:11
- Lesson 2.24: **Creation of BCP and DRP (CYBRScore LAB)**
- Lesson 2.25: Developing the Teams 04:19
- Lesson 2.25: Types of Tests 08:55

Module 3 | Asset Security

- Lesson 3.1: Introduction to Asset Security (01:48)
- Lesson 3.2: Data Classification (05:48)
- Lesson 3.3: Data Protection (10:17)
- Lesson 3.4: System Hardening and Baselining (08:23)
- Lesson 3.5: Threats to Data Storage (12:56)
- Lesson 3.6: Data Redundancy (06:13)
- Lesson 3.7: Secure Data Disposal (06:07)

Module 4 | Security Engineering and Architecture

- Lesson 4.1: Cryptography Agenda (04:27)
- Lesson 4.2: Cryptography in History (14:30)
- Lesson 4.3: Security Services Provided by Cryptography (11:00)
- Lesson 4.4: Algorithm (14:02)
- Lesson 4.5: Elements of Cryptography Part 1 (08:56)

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Lesson 4.6: Elements of Cryptography Part 2 (09:55)

Lesson 4.7: Principles of Secure Design (11:01)

Lesson 4.8: Security Models Part 1 (15:31)

Lesson 4.9: Security Models Part 2 (09:56)

Lesson 4.10: Security Models Part 3 (09:06)

Lesson 4.11: Security Models Part 4 (12:41)

Lesson 4.12: System Architecture (10:46)

Lesson 4.13: Evaluation Criteria Part 1 (08:22)

Lesson 4.14: Evaluation Criteria Part 2 (11:12)

Module 5 | Communications and Network Security

Lesson 5.1: Introduction to Communications and Network Security (08:52)

Lesson 5.2: The OSI Model Part 1 (13:15)

Lesson 5.3: The OSI Model Part 2 (09:22)

Lesson 5.4: The OSI Model Part 3 (07:39)

Lesson 5.5: The OSI Model Part 4 (06:17)

Lesson 5.6: The OSI Model Part 5 (11:47)

Lesson 5.7: The OSI Model Network Devices (08:58)

Lesson 5.8: The OSI Model Collision Domains (08:50)

Lesson 5.9: The OSI Model Layer 3 Protocols (10:38)

Lesson 5.10: The OSI Model Layer 4 (12:22)

Lesson 5.11: The OSI Model Layers 5 and 6 (02:44)

Lesson 5.12: The OSI Model Layer 7 (06:53)

Lesson 5.13: The OSI Model Firewalls Part 1 (07:26)

Lesson 5.14: The OSI Model Firewalls Part 2 (08:35)

Lesson 5.15: The OSI Model Firewalls Part 3 (10:12)

Lesson 5.16: The OSI Model NAT/PAT (08:43)

Lesson 5.17: Password Security (02:13)

Lesson 5.18: Area Networks - LAN, WAN, and MAN (10:34)

Lesson 5.19: Remote Access (10:04)

Lesson 5.20: General Routing Encapsulation (03:31)

Lesson 5.21: Wireless Security Part 1 (08:14)

Lesson 5.22: Wireless Security Part 2 (05:43)

Lesson 5.23: Wireless Security Part 3 (05:30)

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Module 6 | Identity and Access Management

- Lesson 6.1: Introduction to Identity and Access Management Part 1 (10:48)
- Lesson 6.2: Introduction to Identity and Access Management Part 2 (10:54)
- Lesson 6.3: Authentication Types Part 1 - Something You Know (04:21)
- Lesson 6.4: Authentication Types Part 2 - Token Devices (06:08)
- Lesson 6.5: Authentication Types Part 3 - Memory Cards (05:02)
- Lesson 6.6: Authentication Types Part 4 - Something You Are (03:55)
- Lesson 6.7: Strong Authentication (03:31)
- Lesson 6.8: Social Media and the Introduction to Kerberos (05:53)
- Lesson 6.9: Kerberos Components (07:59)
- Lesson 6.10: The Kerberos Carnival Part 1 (11:29)
- Lesson 6.11: The Kerberos Carnival Part 2 (09:56)

Module 7 | Security Assessment and Testing

- Lesson 7.1: The 6 Security Assessments and Testing Objectives (01:55)
- Lesson 7.2: Vulnerability Assessments and Penetration Testing (07:42)
- Lesson 7.3: Vulnerability Scanning (05:57)
- Lesson 7.4: Testing Guidelines (04:30)
- Lesson 7.5: Rules of Engagement Part 1 (07:43)
- Lesson 7.6: Rules of Engagement Part 2 (08:49)
- Lesson 7.7: Protocol Analyzers (Sniffers) and Privacy (11:16)
- Lesson 7.8: IDS Part 1 (09:55)
- Lesson 7.9: IDS Part 2 (10:31)
- Lesson 7.10: IDS Part 3 (10:42)

Module 8 | Security Operations

- Lesson 8.1: Security Incident Response (12:16)
- Lesson 8.2: The Forensics Investigation Process Part 1 (07:37)
- Lesson 8.3: The Forensics Investigation Process Part 2 (07:20)
- Lesson 8.4: Evidence Types (08:38)
- Lesson 8.5: Fault Management (10:02)
- Lesson 8.6: Backups (08:36)

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Module 9 | Software Development Security

- Lesson 9.1: Introduction to Software Development Security (07:44)
- Lesson 9.2: Secure Design (04:37)
- Lesson 9.3: Requirements to Writing Secure Code (03:25)
- Lesson 9.4: Software Development Methodologies (06:25)
- Lesson 9.5: Cloud Application Security (03:24)
- Lesson 9.6: OWASP (10:35)
- Lesson 9.7: Organizational Normative Framework (09:31)
- Lesson 9.8: Object Oriented Programming (07:57)
- Lesson 9.9: Database Introduction Part 1 (02:55)
- Lesson 9.10: Database Introduction Part 2 (12:20)
- Lesson 9.11: Database Introduction Part 3 (07:43)
- Lesson 9.12: Database Introduction Part 4 (04:13)
- Lesson 9.13: Database Introduction Part 5 (07:46)
- Lesson 9.14: Database Introduction Part 6 - Conclusion (07:10)
- Lesson 9.15: **ISC2 CISSP Practice Test: Certified Information Systems Security Professional (Kaplan Practice Test)**

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.