CISSP (Certified Information Systems Security Professional, Videos & Skill Labs Set

Course Specifications

Course Number: ACI77-012VL_rev1.0
Video and Lab Length: Approximately 63 hours, 32 minutes

Course Introduction

Across risk management, cryptography, access control, secure network and system administration, vulnerability scanning, incident response concepts, and secure infrastructure configuration—this lab set prepares students for advanced security and CISSP roles.

Video Enhanced Learning

(39h 32m * 9 Modules * 159 Episodes)

We've enhanced select lab sets with targeted video content to strengthen student readiness and improve lab success. With focused video learning, students get reinforcement of core concepts before they enter the lab, giving them the confidence and context needed to apply skills effectively. Support diverse learning styles, improve lab readiness, and drive stronger outcomes across today's most in-demand skills.

Video Topics

1. Course Overview
2. Five Pillars of Information Security
3. Security Concepts for Organizations
4. Security Governance Principles
5. Security Control Frameworks Foundation
6. ISO and NIST Security Control Frameworks
7. Other Security Control Frameworks
8. Legal Systems
9. United States Laws and Regulations
10. International Laws and Regulations
11. Legal, Regulatory, and Compliance Issues
12. Investigation Types
13. Compliance

14. Security Documentation
15. Personnel Policies and Ethics
16. Security Awareness
17. Business Continuity Concepts
18. Business Impact Analysis (BIA)
19. Business Continuity Process
20. Risk Management Concepts
21. Threat and Vulnerability Identification
22. Risk Analysis
23. Risk Response-Treatment
24. Control Implementation
25. Risk Reporting and Continuous Monitoring
26. Risk Frameworks
27. Threat Modeling
28. Supply Chain Risk Management
29. Asset Classification
30. Data Classification
31. Information and Asset Handling
32. Provisioning Information and Assets
33. Data Roles
34. Data Lifecycle Phases
35. Asset Retention
36. Data States
37. Scoping and Tailoring
38. Standards Selection
39. Data Protection Methods
40. Using Secure Design Principles
41. Security Model Basics
42. Security Modes
43. Security Model Types
44. Bell-LePadula
45. Biba
46. Clark-Wilson
47. Other Security Models

48. Choosing Security Controls
49. Memory Protection
50. Trusted Platform Module
51. Encryption and Decryption
52. Client Vulnerabilities
53. Server Vulnerabilities
54. Database Vulnerabilities
55. Cloud Vulnerabilities
56. Industrial Control System Vulnerabilities
57. IoT Embedded and Edge Computing Vulnerabilities
58. Virtualization and Container Vulnerabilities
59. Distributed Microservices and Serverless Vulnerabilities
60. High Performance Computing Vulnerabilities
61. Cryptography Basics
62. PKI
63. Digital Signatures
64. Classic Cryptanalyic Attacks
65. Side Channel Attacks
66. Other Cryptanalytic Attacks
67. Secure Site and Facility Design Basics
68. Utilizing Natural Access Controls
69. Planning for Physical Security
70. Common Types of Facilities and Sites
71. Facilities and Sites Security Controls
72. Information System Life Cycle Management
73. Video, Voice and Collaboration Technologies
74. OSI and TCP-IP Models
75. Network Transmission Media
76. Transport Architecture
77. Multilayer and Converged Protocols
78. Network Performance Metrics and Traffic Flows
79. Data and Third-party Communications
80. Endpoint Security
81. Monitoring and Management Technologies

82. IPv4 Addressing Protocol
83. Remote Access Technologies
84. Virtual Private Clouds
85. Wireless Network Security
86. Cellular and Satellite Communications
87. Micro-segmentation
88. Edge Networks and CDNs
89. Wireless Network Architecture
90. Operations of Infrastructure
91. Software Defined Networking
92. Secure Protocol Implementations
93. Physical and Logical Network Segmentation
94. IPv6 Addressing Protocol
95. Network Access Control Systems
96. Control Physical and Logical Access
97. Type of Access Controls
98. Groups and Roles
99. AAA
100. Session Management
101. Registration and Proofing
102. FIM
103. Credential Management
104. SSO and Just-in-TIme
105. Role-Rule Based Access Control
106. MAC-DAC
107. Other Access Control Methods
108. Access Policy Enforcement
109. Account Access Review
110. Provisioning-Deprovisioning
111. Role Definition - Privilege Escalation
112. Service Accounts Management
113. OAuth-OIDC
114. SAML-Kerberos
115. RADIUS-TACACS+

116. Designing Security Tests
117. Vulnerability Assessments
118. Penetration Testing
119. Other Common Tests
120. Collecting Security Process Data
121. Analyzing Test Output
122. Conducting Security Audits
123. Understand and Comply with Investigations
124. Logging and Monitoring Activities
125. Configuration Management
126. Foundational Security Operations Concepts
127. Apply Resource and Media Protection
128. Conduct Incident Management
129. Detection and Preventative Measures
130. Implement Patch and Vulnerability Management
131. Change Management Processes
132. Implement Recovery Strategies
133. Implement Disaster Recovery Processes
134. Test Disaster Recovery Plan
135. Business Continuity Planning
136. Implement and Manage Physical Security
137. Personnel Safety and Security
138. Introducing software development security
139. Choosing a software development methodology
140. Considering process driven methodologies
141. Considering agile based methodologies
142. Integrating the capability maturity model in the SDLC
143. Adopting SAMM Into your software development
144. Improving product with an integrated product team
145. Managing post-deployment product expectations
146. Introducing security controls in software development
147. Minimizing programming language risks in the sdlc
148. Developing, deploying, and maintaining secure software
149. Integrating software configuration management

150. Incorporating application security testing
151. Implementing auditing and logging of software changes
152. Focusing on risk analysis and mitigation in the SDLC
153. Evaluating COTS and third-party software security
154. Evaluating managed service and open source software security
155. Evaluating cloud services security
156. Identifying security flaws at source-code level
157. Introducing coding languages and tools
158. Securing APIs
159. Integrating sdn and sdsec

Skill Labs

(24h * 24 Labs)

A **skills lab** is a guided, hands-on learning environment that allows students to practice real-world tasks in a safe, virtual setting. Instead of simply reading or watching videos, learners actively do the work—navigating realistic scenarios, applying concepts, troubleshooting issues, and building confidence through practical experience. This ensures that theory becomes usable skill. Skill labs are essential for developing true workplace readiness because they mirror real systems, tools, and challenges, helping learners bridge the gap between knowledge and performance. By completing a skills lab, students gain the hands-on competence employers expect and are better prepared for both assessments and real job responsibilities.

Skill Labs Topics

1. Introduction to CISSP (ISC2-CISSP)
2. Security and Risk Management (ISC2-CISSP)
3. Encryption and Hashing (ISC2-CISSP)
4. SCCM Configuration Items and Baselines (ISC2-CISSP)
5. Implement OpenPGP (ISC2-CISSP)
6. Two Factor Authentication with SSH (ISC2-CISSP)
7. Implement SSL VPN using ASA Device Manager (ISC2-CISSP)
8. Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering (ISC2-CISSP)
9. Configuring IPtables (ISC2-CISSP)
10. Windows Command Line Tools (ISC2-CISSP)
11. Administering and Deploying Endpoint Protection (ISC2-CISSP)
12. BitLocker on Portable Media (ISC2-CISSP)

13. Managing Remote Desktop (ISC2-CISSP)
14. Manage Role-Based Security (ISC2-CISSP)
15. Configuring MBSA Scanner (ISC2-CISSP)
16. Compliance Patching (ISC2-CISSP)
17. Passive Topology Discovery (ISC2-CISSP)
18. Scanning and Remediating Vulnerabilities with OpenVAS (ISC2-CISSP)
19. Installing Kali (ISC2-CISSP)
20. Implement Backup and Recovery (ISC2-CISSP)
21. Installation and Verification of Snort (ISC2-CISSP)
22. Configuring and Securing IIS (ISC2-CISSP)
23. Upgrading and Securing SSH Connection (ISC2-CISSP)
24. DVWA - Manual SQL Injection and Password Cracking (ISC2-CISSP)