CISSP CERTIFICATION PREP COURSE V1.0

DURATION: 5 DAYS

COURSE OVERVIEW

Gain core knowledge and experience to successfully implement and manage security programs and prepare for the CISSP certification. This course is the most comprehensive review of information security concepts and industry best practices, and focuses on the eight domains of the CISSP CBK (Common Body of Knowledge) that are covered in the CISSP exam. You will gain knowledge in information security that will increase your ability to successfully implement and manage security programs in any organization or government entity.

Why take the CISSP Certification Prep Course?

The CISSP exam is challenging, but the benefits are immense. Due to its comprehensive breadth, CISSP is the de facto certification to show competence in cyber roles. It is also one of the top-paying certifications in IT.

This course supports a certification that is a DOD Approved 8570 Baseline Certification and meets DoD 8140/8570 training requirements.

TARGET AUDIENCE

Individuals looking to establish information security best practices within their organizations or those looking to advance their career within the information security arena.

COURSE OBJECTIVES

After completing this course you should have an in-depth understanding of the eight fundamental domains of information security:

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing

7. Security Operations
8. Software Development Security

COURSE CONTENT

Security and Risk Management (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity)

1. Understand and Apply Concepts of Confidentiality, Integrity, and Availability
2. Apply Security Governance Principles
3. Compliance
4. Understand Legal and Regulatory Issues that Pertain to Information Security in a Global Context
5. Develop and Implement Documented Security Policy, Standards, Procedures, and Guidelines
6. Understand Business Continuity Requirements
7. Contribute to Personnel Security Policies
8. Understand and Apply Risk Management Concepts
9. Understand and Apply Threat Modeling
10. Integrate Security Risk Considerations into Acquisitions Strategy and Practice
11. Establish and Manage Security Education, Training, and Awareness
12. Asset Security (Protecting Security of Assets)
13. Classify Information and Supporting Assets
14. Determine and Maintain Ownership
15. Protect Privacy
16. Ensure Appropriate Retention
17. Determine Data Security Controls
18. Establish Handling Requirements
19. Security Engineering (Engineering and Management of Security)
20. Implement and Manage an Engineering Life Cycle Using Security Design Principles
21. Understand Fundamental Concepts of Security Models
22. Select Controls and Countermeasures Based Upon Information Systems Security Standards
23. Understand the Security Capabilities of Information Systems
24. Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements

25. Assess and Mitigate Vulnerabilities in Web-based Systems
26. Assess and Mitigate Vulnerabilities in Mobile Systems
27. Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems
28. Apply Cryptography
29. Apply Secure Principles to Site and Facility Design
30. Design and Implement Facility Security
31. Communications and Network Security (Designing and Protecting Network Security)
32. Apply Secure Design Principles to Network Architecture
33. Securing Network Components
34. Design and Establish Secure Communication Channels
35. Prevent or Mitigate Network Attacks
36. Identity and Access Management (Controlling Access and Managing Identity)
37. Control Physical and Logical Access to Assets
38. Manage Identification and Authentication of People and Devices
39. Integrate Identity as a Service (IDaaS)
40. Integrate Third-Party Identity Services
41. Implement and Manage Authorization Mechanisms
42. Prevent or Mitigate Access Control Attacks
43. Manage the Identity and Access Provisioning Life Cycle
44. Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
45. Design and Validate Assessment and Test Strategies
46. Conduct Security Control Testing
47. Collect Security Process Data
48. Conduct or Facilitate Internal and Third-Party Audits
49. Security Operations (e.g., Foundational Concepts, Investigations, Incident Management, Disaster Recovery)
50. Understand and Support Investigations
51. Understand Requirements for Investigation Types
52. Conduct Logging and Monitoring Activities
53. Secure the Provisioning of Resources through Configuration Management
54. Understand and Apply Foundational Security Operations Concepts
55. Employ Resource Protection Techniques
56. Conduct Incident Response

57. Operate and Maintain Preventative Measures
58. Implement and Support Patch and Vulnerability Management
59. Participate in and Understand Change Management Processes
60. Implement Recovery Strategies
61. Implement Disaster Recovery Processes
62. Test Disaster Recovery Plan
63. Participate in Business Continuity Planning
64. Implement and Manage Physical Security
65. Participate in Personnel Safety
66. Software Development Security (Understanding, Applying, and Enforcing Software Security)
67. Understand and Apply Security in the Software Development Life Cycle
68. Enforce Security Controls in the Development Environment
69. Assess the Effectiveness of Software Security
70. Assess Software Acquisition Security

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

1. A minimum of 5 years' experience working in IT infrastructure and Cybersecurity

TEST CERTIFICATION

Recommended as preparation for the following exams:

- CISSP – Certified Information Systems Security Professional

To qualify for this cybersecurity certification, you must pass the exam and have at least five years of cumulative, paid work experience in two or more of the eight domains of the (ISC) ² CISSP Common Body of Knowledge (CBK).

It may be possible to satisfy one year of required work experience with a relevant four-year college degree or if you hold an approved credential.

Even if you don't have the required level of experience you can still pass the CISSP exam and become an associate of (ISC) ² while you earn the required work experience.