



Certified Information Systems Security Professional (CISSP)

CISSP Overview

Businesses make substantial investments in information assets, including technology, architecture, and processes. These assets are protected on the strengths of the professionals in charge.

Industry standards, ethics and certification of IS professionals becomes critical to ensuring that higher standards for security are achieved. Training for the CISSP exam covers all ten domains of the Common Body of Knowledge.

This course should be attended by network and firewall administrators, information security officers, and anyone interested in understanding the principles, best practices, and core concepts of information systems security.

Course Overview

CISSP training is an advanced course designed to meet the high demands of the information security industry by preparing students for the Certified Information Systems Security Professional (CISSP) exam. This certification is managed by the internationally recognized and highly prestigious International Information Systems Security Certifications Consortium ISC².

The exam covers ISC²'s ten domains from the Common Body of Knowledge (CBK), encompassing the whole of information security. The exam consists of 250 multiple-choice questions. Candidates have up to 6 hours to complete the examination.

Course materials reflect the latest information system security issues, concerns, and countermeasures.

- Discusses all ten domains of Common Body of Knowledge (CBK), helping to prepare for the CISSP exam.
- The CBK is the compilation and distillation of all information systems security material collected internationally of relevance to information system security professionals.



- Ensures information system security professionals have an opportunity to review the CBK in-depth, in preparation for the certification examination and to stay current on the ever-evolving domains within the information system security field.
- Presents a high-level review of the main topics
- Identifies specific areas students should study for exam preparation
- Provides an overview of the scope of the field

Course Topics

1. Security Management Practices

- Security management concepts
- Policies, standards, guidelines, and procedures
- Security awareness concepts
- Risk management practices
- Basic information on classification levels

Security management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines.

Management tools such as data classification and risk assessment and analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented.

2. Access Control Systems

Access controls are a collection of administrative, physical, and technical mechanisms that work together within a security architecture to protect the assets of an information system. Coverage of the threats, vulnerabilities, and risks associated with an information system's infrastructure, and the available preventive and detective measures to counter them.



3. Telecommunications, Network, and Internet Security

- Network Structures
- Transmission methods
- Transport formats
- Security measures providing availability, integrity, and
- Authentication for transmissions over public and private networks

4. Cryptography

Addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

- Definitions
- History
- Cryptology Fundamentals
- Symmetric Key Cryptosystem Fundamentals
- Asymmetric Key Cryptosystem Fundamentals
- Key Distribution and Management Issues
- Public Key Infrastructure Definitions and Concepts

5. Security Architecture and Models

Concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of confidentiality, availability, and integrity.

- Computer organization
- Hardware components
- Software/firmware components
- Open systems
- Distributed systems
- Protection mechanisms
- Evaluation criteria
- Certification and accreditation
- Formal security models
- Confidentiality models
- Integrity models
- Information flow models



6. Operations Security

Identifies the controls over hardware and media, and the operators and administrators with access privileges to any of these resources. Auditing and monitoring provide the mechanisms, tools, and facilities that permit the identification of security events. Subsequent actions identify key elements and report pertinent information to the appropriate individual, group, or process.

7. Applications and Systems Development Security

Addresses the important security concepts that apply to application software development. Outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.

- The software development life cycle
- Object-oriented systems
- Artificial intelligence systems
- Database security issues
- Data warehousing Data mining
- Application controls

8. Business Continuity Planning and Disaster Recovery Planning

Addresses the preservation and recovery of business operations in the event of outages. Differences between business continuity planning and disaster recovery.

- Project scope and planning, business impact analysis
- Recovery strategies
- Recovery plan development
- Implementation
- Recovery plan development, implementation and restoration

9. Law, Investigations, and Ethics

- Computer crime laws and regulations
- The measures and technologies used to investigate computer crime incidents
- Laws applying to computer crimes
- How to determine if a crime has occurred
- Preserving evidence
- The basic of conducting an investigation
- Liabilities under the law



10. Physical Security

Provides protection techniques for the entire facility, from the outside perimeter to inside office space, including all information system resources.

- Elements involved in choosing a secure site, its design and configuration
- Methods for securing a facility against unauthorized access
- Methods for securing the equipment against theft of the equipment or its contained information
- Environmental and safety measures needed to protect personnel, the facility and its resources

CISSP Prerequisites

To become a CISSP, a candidate must successfully complete two processes, Examination and Certification:

Examination

- The eligibility requirements to sit for the CISSP examination are completely separate from the eligibility requirements necessary to be certified.
- To sit for the CISSP examination, a candidate must:
- Submit the examination fee.
- Assert that he or she possesses a minimum of four years of professional experience in the information security field. (or three years plus a college degree for prospective candidates effective January 01, 2003).
- Complete the Candidate Agreement, attesting to the truth of his or her assertions regarding professional experience and legally commit to adhere to the CISSP Code of Ethics.
- Successfully answer four questions regarding criminal history and related background.

Certification

To be issued a certificate, a candidate must:

- Pass the CISSP exam with a scaled score of 700 points or greater.
- Submit a properly completed and executed Endorsement Form.



- If the candidate is selected for audit, they must successfully pass that audit of their assertions regarding professional experience.
- Endorsement

- Once a candidate has been notified of passing the CISSP examination, he or she will be required to have his or her application endorsed by a CISSP before the credential can be awarded. If no CISSP can be found, another qualified professional with knowledge of information systems or an officer of the candidate's corporation can be used to validate the candidate's professional experience.

- The endorser will attest that the candidate's assertions regarding professional experience are true to the best of their knowledge, and that the candidate is in good standing within the information security industry.

- Upon receipt of the Endorsement Form and barring a random audit of the candidate's professional experience, the CISSP credential should be awarded within one business day, with a formal notification sent via e-mail.

Audit

- A percentage of the candidates who pass the CISSP examination and submit endorsements will be randomly subjected to audit and required to submit a resume for formal review and investigation.

- If audited (subject to results), the credential will be awarded within seven business days and notification sent via e-mail. Naturally, there may be some delays due to mail service or the number of forms received. Also, audits may require additional time for verifying information and/or contacting references.

Current skill sets

- Knowledge and experience with several of the following general security areas:
 - Designing, implementing and maintaining firewalls
 - auditing, intrusion detection systems
 - access control lists
 - availability strategies
 - discretionary access lists
 - biometric devices
 - certificates
 - disaster recovery



Target Audience

- Security Officers
- Application Developers
- Network Administrators
- Network Managers
- Risk Managers
- Attorneys