

CISSP – Certified Information System Security Professional

Course Acronym: CISSP
Course Length: 5 days

Who should attend

This course is designed for Networking Security Professionals who wish to attain CISSP certification and facilitate their growth as a security professional.

Content

Security Management Practices

- A Concepts of confidentiality, integrity and Availability
- B Security threats, safeguards, vulnerabilities and attacks
- C Risk management processes
- D Building blocks of information security
- E Security awareness programs
- F IS audit process

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/analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented.

Security Architecture & Models

- A Common computer and network concepts, architecture and design
- B Common security models, architecture and evaluation criteria
- C common flows and security issues associated with system architecture and designs
- D Business systems and processes evaluation techniques

The Security Architecture and Models domain contains the 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 availability, integrity, and confidentiality.

Access Control Methodology

- A Access control models, methodologies and techniques
- B Access control administration practices
- C Identification and authentication techniques
- D Methods of attack to access control systems
- E the concept of penetration testing

Access controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.

Application Development Security

This domain addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.

Technical Infrastructure, Operational Practices & Operation Security

- A Information systems operation practices
- B Control over hardware, media and operations control mechanisms
- C Problem and performance monitoring tools and techniques

Operations Security is used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

Physical Security

The physical security domain provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources. Business Continuity Planning and Disaster

Cryptography

The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

Telecommunications, Network, and Internet Security

The telecommunications, network, and Internet security domain discusses the:

- Network Structures
- Transmission methods
- Transport formats
- Security measures used to provide availability, integrity, and confidentiality
- Authentication for transmissions over private and public communications networks and media.

Business Continuity Planning

- A The concept of business continuity planning and disaster recovery
- B The business continuity planning process covering project scope and planning, business impact analysis and recovery
- C The disaster recovery process in terms of recovery plan development, implementation and restoration
- D The techniques in auditing a business continuity plan

The Business Continuity Plan (BCP) domain addresses the preservation and recovery of business operations in the event of outages.

Law, Investigations, and Ethics

The Law, Investigations, and Ethics domain addresses:

- Computer crime laws and regulations
- The measures and technologies used to investigate computer crime incidents

Even though the curriculum and CBK were developed in the United States, the material does not boast a definite US flavor. The material and the exam, focuses on international issues.