



CISSP® Certification Training

Overview

This course provides a comprehensive discussion of the ten core subject areas fundamental to the understanding of security for CIOs, managers, and engineers. This course covers the ten domains that are required knowledge for the CISSP® certification exam.

Outline

Lesson 1: Access Control Systems & Methodology

Requires that the candidate understands the concepts, systems and methodologies involved in granting and restricting access to resources.

Lesson 2: Applications & Systems Development

Requires that the candidate understands the security controls found in systems and application software, such as the affects of malicious code on distributed application environments and the security controls involved in data warehousing.

Lesson 3: Business Continuity & Disaster Recovery Planning

Involves the preparation planning and updating of specific actions to protect mission critical services and data.

Lesson 4: Cryptography

This domain addresses the concepts, means and methods of the encrypting data to ensure authenticity, integrity, and confidentiality.

Lesson 5: Law, Investigation & Ethics

Pertains to computer crime laws, methods for gathering evidence, and related ethical issues.

Lesson 6: Operations security (Computer)

Identifies the controls over hardware, media

and the operators of these resources, and issues related to auditing and monitoring.

Lesson 7: Physical Security

Involves the threats, vulnerabilities and countermeasures utilized to physically protect enterprises' resources.

Lesson 8: Security Architecture & Models

This domain engages in the design, concepts, standards, and implementation security measures that ensure the availability, integrity and confidentiality of operating systems, applications and equipment.

Lesson 9: Security Management Practices

Manages the identification of a company's information assets, and the development, documentation and implementation of security policies.

Lesson 10: Telecommunications & Network Security

This domain involves designing and planning voice and data infrastructure and communications with a security strategy that includes preventative, detective and corrective measures.

Attendee Profile

The CISSP program is targeted at mid-to-senior level professionals who possess at least four (4) years of experience in the information security field or three (3) years of experience and a college degree. 2 months of pre-study is recommended.



Logistics

Five (5) day training program