Certified Information Systems Security Professional (CISSP)

Length: 5 Days

Type: Course

Delivery Method: Instructor-led (classroom)

About

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the not-for-profit International Information Systems Security Certification Consortium, (ISC)2.

The CISSP certification was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. It is approved by the U.S. Department of Defense (DoD) in both their Information Assurance Technical (IAT) and Managerial (IAM) categories. CISSP certified professionals are considered authorities on key security issues including mobile security, risk management, application development security, cloud computing, among others.

Public

The CISSP training is ideal for the following professionals:

- Chief Information Security Officers (CISO)
- IT Directors
- IT Security Consultants/Managers
- Security Architects/Auditors
- IT Managers
- Security System Engineers
- Network Architects



Objectives

- Understand the basics of telecommunication and network security concepts, required components for minimizing security risks, securing channels of communication, and techniques for preventing and detecting network-based attacks.
- Identify the key terms and processes of security operations and how to protect and control information processing assets in a centralized or distributed environment in this CISSP training.
- Define and apply information security governance and Risk Management Framework including the policies, concepts, principles, structures and standards that are established for the protection of information assets and how to assess the effectiveness of that protection
- Gain the required skills to design the architecture and manage IT security in an enterprise environment through this authorized CISSP course

Course Content

Domain 1: Security and Risk Management (Security, Risk, Compliance, Law, Regulations, and Business Continuity)

- Confidentiality, integrity, and availability concepts
- Security governance principles
- Compliance
- Legal and regulatory issues
- Professional ethic
- Security policies, standards, procedures and guidelines

Domain 2: Asset Security (Protecting Security of Assets)

- Information and asset classification
- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)

Domain 3: Security Engineering (Engineering and Management of Security)

- Engineering processes using secure design principles
- Security models fundamental concepts
- Security evaluation models
- Security capabilities of information systems
- Security architectures, designs, and solution elements vulnerabilities
- Web-based systems vulnerabilities
- Mobile systems vulnerabilities
- Embedded devices and cyber-physical systems vulnerabilities
- Cryptography
- Site and facility design secure principles
- Physical security

Domain 4: Communication and Network Security (Designing and Protecting Network Security)

- Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
- Secure network components
- Secure communication channels
- Network attacks

Domain 5: Identity and Access Management (Controlling Access and Managing Identity)

- Physical and logical assets control
- Identification and authentication of people and devices
- Identity as a service (e.g. cloud identity)
- Third-party identity services (e.g. on-premise)
- Access control attacks
- Identity and access provisioning lifecycle (e.g. provisioning review)

Domain 6: Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

- Assessment and test strategies
- Security process data (e.g. management and operational controls)
- Security control testing
- Test outputs (e.g. automated, manual)
- Security architectures vulnerabilities

Domain 7: Security Operations (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)

- Investigations support and requirements
- Logging and monitoring activities
- Provisioning of resources
- Foundational security operations concepts
- Resource protection techniques
- Incident management
- Preventative measures
- Patch and vulnerability management



- Change management processes
- Recovery strategies
- Disaster recovery processes and plans
- Business continuity planning and exercises
- Physical security
- Personnel safety concerns

Domain 8: Software Development Security (Understanding, Applying, and Enforcing Software Security)

- Security in the software development lifecycle
- Development environment security controls
- Software security effectiveness
- Acquired software security impact