Certified Information Systems Security Professional (CISSP®)

Duration: 5 Days
Method: Instructor-Led

Certification: Certified Information Systems Security Professional (CISSP®)

Course Description

The CISSP® certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks. Backed by (ISC)²®, the globally recognized, not-for-profit organization dedicated to advancing the information security field, the CISSP® was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP® an objective measure of excellence, but also a globally recognized standard of achievement.

Target Audience

This course is aimed at:

- Security Consultants
- Security Managers
- IT Directors/Managers
- Security Auditors
- Security Architects
- Security Analysts
- Security Systems Engineers
- Chief Information Security Officers
- Directors of Security
- Network Architects

Prerequisites

Before attending this course, candidates should have the following:

- Minimum of five (5) years cumulative paid full-time work experience in two (2) or more of the eight (8) domains of the CISSP® Common Body of Knowledge (CBK) shown in the Course Content

Course Objectives

Upon completion of the course, candidates will have the knowledge and skills to:

- Understand and apply the concepts of risk assessment, risk analysis, data classification, and security awareness and Implement risk management and the principles used to support it (Risk avoidance, Risk acceptance, Risk mitigation, Risk transference)
- Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and address the frameworks and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets, as well as to assess the effectiveness of that protection and establish the foundation of a comprehensive and proactive security program to ensure the protection of an organization’s information assets
- Apply a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel, and organizational sub-units so that these practices and processes align with the organization's core goals and strategic direction and examine the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality, and authenticity
- Understand the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media and identify risks that can be quantitatively and qualitatively measured to support the building of business cases to drive proactive security in the enterprise.
- Offer greater visibility into determining who or what may have altered data or system information, potentially affecting the integrity of those asset and match an entity, such as a person or a computer system, with the actions that entity takes against valuable assets, allowing organizations to have a better understanding of the state of their security posture.
- Plan for technology development, including risk, and evaluate the system design against mission requirements, and identify where competitive prototyping and other evaluation techniques fit in the process
- Protect and control information processing assets in centralized and distributed environments and execute the daily tasks required to keep security services operating reliably and efficiently.
- Understand the Software Development Life Cycle (SDLC) and how to apply security to it, and identify which security control(s) are appropriate for the development environment, and assess the effectiveness of software security

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
"Training You Can Really Use"

Course Content

Domain 1: Security and Risk Management

- 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

- 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 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

Domain4: Communication and 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

- 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

- 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

- 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

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

CompTIA AUTHORIZED PARTNER PROGRAM
Microsoft Partner Silver Learning
PROMETRIC
EC-Council Accredited Training Center