8 Days

CISSP - Certified Information Systems Security Professional

CISSP training (Certified Information Systems Security Professional) prepares you for the most sought-after certification. **CISSP certification** is the essential credential for a security professional to validate their competencies and skill set to deploy a diverse information security infrastructure for protecting the organization from potential cybersecurity hazards.

CISSP Training and certification qualifies a candidate to effectively create, implement, and evaluate the cybersecurity tools and technologies used to facilitate the healthy transfer of information across a diverse work environment.

The **CISSP Certification** has been the first credential in the field of information security to meet the stern requirements of ISO/IEC Standard 17024.

CISSP Training from Mercury Solutions is highly interactive and engaging and provides comprehensive knowledge for participants who wish to gain expertise in defining the architecture, design, management, and controls leading to a secure business enterprise. Professionals who attains **CISSP Certification** are high-in-demand by organizations all across the world who needed protecting their organizations from growing vulnerabilities and malicious attacks.

Course Details

Course Outline

DOMAIN	% on 2015 CBK®	% on April 201
Security and Risk Management	16%	15%
Asset Security	10%	10%
Security Architecture and Engineering	12%	13%
Communications and Network Security	12%	14%
Identity and Access Management (IAM)	13%	13%
Security Assessment and Testing	11%	12%
Security Operations	16%	13%
Software Development Security	10%	10%

Domain 1: Security and Risk Management

- Legal and regulatory issues
- Confidentiality, integrity, and availability concepts

- Security governance principles
- Compliance
- Professional ethics
- Business continuity requirements
- Personnel security policies
- Threat modeling
- Risk considerations
- Security education, training, and awareness
- Security policies, standards, procedures and guidelines

Domain 2: Asset Security

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

Domain 3: Security Architecture and Engineering

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

Domain 4: Communication and Network Security

- Secure network architecture design
- Secure communication channels
- Secure network components
- Network attacks

Domain 5: Identity and Access Management (IAM)

- Management of physical/logical access to assets
- Management of identification and authentication
- Integrate identity as a third party service
- Authorization mechanism
- Identity and access of provisioning life cycle

Domain 6: Security Assessment and Testing

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

Domain 7: Security Operations

- Logging and monitoring activities
- Investigations support and requirements
- Incident management
- Provisioning of resources
- Foundational security operations concepts
- Recovery strategies
- Resource protection techniques
- Physical security
- Preventative measures
- Patch and vulnerability management
- Change management processes
- Business continuity planning and exercises
- Personnel safety concerns
- Disaster recovery processes and plans

Domain 8: Software Development Security

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

Who Should Attend

The CISSP certification is ideal for those working with the profiles of:

- Security Systems Engineer
- Security Consultants/Analysts
- Security/Network Architect
- Security Auditor/Manager

Pre Requisite

The candidates must meet the following CISSP Certification prerequisites:

Have a minimum of five years of direct full-time security professional work experience in the below-mentioned domains:

- Access Control
- Cryptography
- Application Development Security
- Operations Security
- Information Security Governance and Risk Management
- Legal, Regulations, Investigations and Compliance
- Business Continuity and Disaster Recovery Planning
- Security Architecture and Design
- Telecommunications and Network Security
- Physical (Environmental) Security

OR

- 4 years of direct full-time security professional work experience in two or more of the ten mentioned domains with a college degree.
- Complete the Candidate Agreement, attesting to the truth of his or her declaration regarding professional experience and legally commit to adhere to the (ISC) 2 Code of Ethics.

Exams

ISC2 Certified Information Systems Security Professional (CISSP) [CISSP]

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India | +91 8882 233 777 | training@mercury.co.in | www.mercurysolutions.co

Date - Apr 24, 2024