BLUEMARK ACADEMY

CISSP (Certified Information Systems Security Professional) Training

Duration: 5 Days · **Training format:** Virtual Classroom / Online

Description

This CISSP training program is designed for experienced information security professionals who aim to gain a comprehensive and strategic understanding of enterprise information security management. The training content is fully aligned with the latest ISC2 CISSP Common Body of Knowledge (CBK) and focuses on both managerial and technical aspects of information security. The program supports participants in preparing effectively for the CISSP certification exam while also enabling them to apply best practices within their organizations.

Audience

Information security, cybersecurity, IT risk and audit professionals

Outline

Domain 1 – Security and Risk Management

- Information security principles: confidentiality, integrity, availability
- Security governance and organizational roles
- Risk management concepts and risk assessment methodologies
- Legal, regulatory, and compliance requirements
- Security policies, standards, procedures, and guidelines
- Business continuity and disaster recovery planning
- Professional ethics and security awareness

Domain 2 – Asset Security

- Identification and classification of information assets
- Asset ownership and accountability
- Data lifecycle management
- Data protection requirements
- Data retention, archiving, and disposal

Domain 3 – Security Architecture and Engineering

- Secure design principles and system architecture
- Security models and system engineering concepts
- Cryptography fundamentals and key management
- Physical and environmental security controls
- Platform and hardware security concepts

Domain 4 – Communication and Network Security

- Network architecture and communication models
- Secure network design and segmentation
- Network protocols and associated security risks
- Network security devices and controls
- Remote access, VPN, and wireless network security

Domain 5 – Identity and Access Management (IAM)

- Identification, authentication, and authorization concepts
- Access control models and mechanisms
- Multi-factor authentication
- Privileged access management
- Identity lifecycle management

Domain 6 – Security Assessment and Testing

- Security assessment and audit processes
- Vulnerability assessment techniques
- Penetration testing concepts
- Security metrics and measurement
- Logging, monitoring, and reporting

Domain 7 – Security Operations

- Operational security processes
- Incident response and handling
- Security Operations Center (SOC) concepts
- Vulnerability, patch, and configuration management
- Digital forensics and post-incident analysis

Domain 8 – Software Development Security

- Secure software development lifecycle (SDLC)
- Application security principles
- Secure coding practices
- Application security testing
- DevSecOps concepts and automation

Prerequisites

Minimum 5 years of experience in information security or IT