Certified Information Security Manager (CISM)

Course Duration: 32 Hours (4 Days)

Overview

The Certified Information Security Manager (CISM) course is a globally recognized certification for information security management professionals. It is designed to ensure that learners have the expertise to establish, manage, and oversee an organization's information security program. Learners will gain a comprehensive understanding of information security governance, risk management, Program development and management, and Incident management. The course is structured into four main modules, each covering critical aspects of information security management. The first module focuses on developing a robust Security governance framework, ensuring management support, and deploying effective strategies. The second module delves into identifying and analyzing risks, as well as monitoring and reporting on them to ensure proper risk management. The third module teaches learners how to align security programs with business objectives, manage resources efficiently, and integrate security into organizational processes. Finally, the fourth module equips learners with the skills to plan for and respond to security incidents, ensuring business continuity and minimizing impact. By completing the CISM course, learners will be well-equipped to take on leadership roles in information security, enhance their professional reputation, and provide significant value to their organizations through effective security management practices.

Audience Profile

The Certified Information Security Manager (CISM) course is designed for IT professionals aiming to manage and oversee enterprise information security.

- Information Security Managers
- IT Auditors
- Risk Managers
- Chief Information Officers (CIOs)
- Chief Information Security Officers (CISOs)
- IT Consultants specializing in information security
- IT Directors or Managers responsible for security
- Security Systems Engineers
- Security Architects and Designers
- IT Professionals aspiring to management roles in Information Security
- Compliance Officers responsible for IT security compliance
- Information Security Analysts
- Network Architects and Engineers focusing on security
- Data Protection Officers (DPOs)

- Privacy Officers
- IT Project Managers involved in security-related projects
- Incident Responders and Incident Handling professionals
- Business Continuity and Disaster Recovery Specialists

Course Syllabus

Domain 1: Information Security Governance

- Organizational Culture
- Legal, Regulatory and Contractual Requirements
- Organizational Structures, Roles and Responsibilities
- Information Security Strategy Development
- Information Governance Frameworks and Standards
- Strategic Planning (e.g., Budgets, Resources, Business Case)

Domain 2: Information Security Risk Management

- Emerging Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment and Analysis
- Risk Treatment / Risk Response Options
- Risk and Control Ownership
- Risk Monitoring and Reporting

Domain 3: Information Security Program

- Information Security Program Resources (e.g., People, Tools, Technologies)
- Information Asset Identification and Classification
- Industry Standards and Frameworks for Information Security
- Information Security Policies, Procedures and Guidelines
- Information Security Program Metrics
- Information Security Control Design and Selection
- Information Security Control Implementation and Integrations
- Information Security Control Testing and Evaluation
- Information Security Awareness and Training
- Management of External Services (e.g., Providers, Suppliers, Third Parties, Fourth Parties)
- Information Security Program Communications and Reporting

Domain 4: Incident Management

- Incident Response Plan
- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Classification/Categorization
- Incident Management Training, Testing and Evaluation
- Incident Management Tools and Techniques
- Incident Investigation and Evaluation
- Incident Containment Methods
- Incident Response Communications (e.g., Reporting, Notification, Escalation)
- Incident Eradication and Recovery
- Post-Incident Review Practices