

Certificate in Information Security Management Principles (CISMP)

Course Duration: 40 Hours (5 Days)

Overview

The Certificate in Information Security Management Principles (CISMP) course is a comprehensive program designed to provide learners with a thorough understanding of information security management. It covers the fundamental principles of securing information systems and managing risks. The course is structured into ten modules, each focusing on a different aspect of information security. Module 1 delves into the core principles of information security management, ensuring learners grasp the basics of protecting Data integrity, Confidentiality, and Availability. Module 2 addresses Information risk, teaching how to identify and mitigate potential Security threats. Module 3 explores various Information security frameworks that guide the establishment of robust Security policies. In Module 4, participants learn about the Security lifecycle, including the phases of planning, implementing, managing, and updating Security measures. Module 5 emphasizes procedural and People security controls, highlighting the human element in safeguarding information. Module 6 focuses on Technical security controls such as Access controls and Cryptography. Module 7 is dedicated to physical and Environmental security controls, stressing the importance of protecting physical assets. Module 8 covers disaster recovery and business continuity management, preparing organizations to respond effectively to incidents. Module 9 looks at other technical aspects, such as network and System security. Finally, Module 10 helps learners prepare for the CISMP examination, consolidating their knowledge and readiness for certification. By completing the CISMP course, learners will gain essential skills in information security management, risk assessment, and the implementation of security controls, all of which are crucial for protecting an organization's data and systems.

Audience Profile

The CISMP course is ideal for professionals seeking a comprehensive understanding of information security management principles.

- IT Managers
- Security Consultants
- IT Professionals looking to transition into information security roles
- Risk Managers
- Compliance Officers
- Privacy Officers
- IT Auditors
- Security Analysts
- Network Administrators

- System Administrators
- Business Analysts involved in security management
- Project Managers overseeing IT projects with a security component
- Corporate Attorneys advising on cybersecurity issues
- Incident Responders and Forensic Analysts
- Security Architects
- Data Protection Officers
- Chief Information Security Officers (CISOs)
- Information Security Officers (ISOs)

Course Syllabus

- **Module 1** – Information Security Management Principles
- **Module 2** – Information Risk
- **Module 3** – Information Security Framework
- **Module 4** – Procedural/People Security Controls
- **Module 5** – Technical Security Controls
- **Module 6** – Software Development and Lifecycle
- **Module 7** - Physical and Environmental Control
- **Module 8** - Disaster Recovery and Business Continuity Management
- **Module 9** – Other technical Aspects
- **Module 10** – Preparation for the CISMP Examination.