# Certified Information Security Manager (CISM)

**Duration: 4 Days**

**Prerequisites:**

To successfully undertake training in the Certified Information Security Manager (CISM) course, the following minimum prerequisites are recommended:

- Basic Understanding of Information Security Concepts:

Familiarity with core information security principles such as confidentiality, integrity, and availability.
Awareness of common security threats and vulnerabilities.

- Foundational IT Knowledge:

General understanding of IT infrastructure components (networks, servers, applications, databases).
Familiarity with IT operations and the role of information security within IT.

- Experience in Information Security or Related Field:

While not mandatory for the course, having some practical experience in information security or a related field such as IT audit, risk management, or information assurance can be beneficial.

- Understanding of Governance and Risk Management:

Basic knowledge of governance principles and the importance of aligning security objectives with organizational goals.
Awareness of risk management processes including risk identification, assessment, and mitigation strategies.

- Professional Experience:

The CISM certification itself requires a minimum of five years of professional information security management experience, but this is not a prerequisite for the training course. However, participants with some level of professional experience may find the course material more relatable.

- Willingness to Learn:

A committed attitude towards learning and understanding complex security management concepts.

- English Proficiency:

Since the training material and the CISM exam are in English, proficiency in reading and understanding technical English is essential.
These prerequisites are aimed at ensuring that participants are adequately prepared to grasp the advanced concepts that will be covered in the CISM Exam Prep Course. However, individuals with a strong desire to learn and improve their information security management skills are encouraged to take the course as it provides a structured learning path towards becoming a CISM.

**Course Description:**

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.

**Target Audience:**

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 Outline:**

Module 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)

Module 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

Module 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

Module 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