CISM Certification Training Course Outline

Duration: 32–40 Hours
Level: Advanced
Delivery Mode: Online / Offline
Certification Body: ISACA
Target Audience: IT Managers, Security Consultants, Risk Officers, CISOs, and Cybersecurity Professionals

---

Module 1: Information Security Governance

- Establishing and Maintaining an Information Security Strategy
- Aligning Security Strategy with Organizational Goals
- Governance Frameworks and Compliance Requirements
- Defining Roles and Responsibilities for InfoSec Governance
- Policies, Standards, and Procedures
- Information Security Governance Metrics

Module 2: Information Risk Management

- Identifying Information Assets and Risk Tolerances
- Risk Assessment and Risk Analysis Techniques
- Risk Register and Risk Prioritization
- Risk Mitigation Strategies and Controls
- Integrating Risk Management into Business Processes
- Business Impact Analysis (BIA)
- Legal, Regulatory, and Contractual Requirements

Module 3: Information Security Program Development and Management

- Establishing and Managing the InfoSec Program
- Resource Allocation and Budgeting
- Security Program Metrics and Reporting
- Developing and Managing Security Policies
- Awareness and Training Programs
- Integrating Security into SDLC and Change Management

- Program Improvement and Performance Monitoring

Module 4: Information Security Incident Management

- Developing and Implementing Incident Response Plans
- Detection, Classification, and Escalation of Security Events
- Response and Recovery Processes
- Post-Incident Analysis and Reporting
- Business Continuity and Disaster Recovery Integration
- Communication with Internal and External Stakeholders
- Legal Considerations in Incident Handling