Certified Information Security Manager (CISM)

Course Duration: 10 Days
Course overview

CISM is an acronym for Certified Information Security Manager. ISACA awards the Certified Information Security Manager **(CISM)** certification to IT professionals who indicate expertise in information security governance, program development & management, incident management, and risk management.

The CISM is a **management-focused certification** that encourages global information security procedures and recognizes professionals' abilities to manage, supervise, and assess an organization's information security.

The CISM certification is designed for those who manage teams of cyber security specialists and others who want to lead security teams.

Course Objectives

1. Understand the roles & responsibilities of a Certified Information Security Manager and how to properly manage a security program.
2. Learn about current security management standards and best practices for Information Security
3. Establish effective security policies, programs and procedures.
4. Develop the skills to create and implement an information security strategy, risk management program and security audit process.
5. Identify, evaluate and mitigate threats to an organization's IT infrastructure, applications and data
6. Know how to ensure that all internal and external stake holders are compliant with security policies and processes.
7. Gain expertise in handling crisis management, incident response and disaster recovery.
8. Understand the importance of effective communications to ensure awareness of the policies and procedures throughout an organization.

CISM Prerequisites

Not every IT professional can take the exam. Someone who aspires to be CISM-certified must have 5 years of experience in information security, with at least 3 years of information security management experience in 3 or more of the CISM domains mentioned above. Moreover, the experience should be gained within 10 years before the application date or within 5 years after passing the exam.

After passing the exam, applicants can then apply for CISM certification within 5 years.

Target Audience

The primary audience for Certified Information Security Manager (CISM) training is security professionals and IT administrators who wish to advance their skills and knowledge in the field of information security.
This type of training is essential for IT professionals who wish to gain a comprehensive understanding of the security risks and approaches that are used to protect businesses and their data.
Those who take CISM training will learn about various areas of security risk management and security controls, as well as how to build and maintain an effective security program.
The training also provides individuals with the skills to develop and evaluate security policies, understand security process and technologies, and manage and monitor an organization's information security program.
CISM training is also beneficial for individuals who are working in the field of information security or those who are pursuing a degree in the respective field.
Ultimately, the CISM certification is an important asset for anyone who wants to increase their credentials in order to advance their career.

Benefits for CISM Certification

1. **Higher Salary**
2. **More Credibility**
3. **More Knowledge**

Course Domains

Domain #	Domain Topic	Domain Description
Domain 01: (17%) Information Security Governance	A. Enterprise Governance	• Organizational Culture • Legal, regulatory, and contractual requirements • Organizational structure, roles and responsibilities
	B. Information Security Strategy	• Information security strategy development • Information governance framework and standards • Strategic Planning (e.g., budgets, resources, business case).
Domain 02: (20%) Information Security Risk Management	A. Information Security Risk Assessment	• Emerging Risk and Threat Landscape • Vulnerability and Control Deficiency Analysis • Risk Assessment and Analysis
	B. Information Security Risk Response	• Risk Treatment / Risk Response Options • Risk and Control Ownership • Risk Monitoring and Reporting
Domain 03: (33%) Information Security Program	A. Information Security Program Development	• 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
	B. Information Security Program Management	• Information Security Control Design and Selection • Information Security Control Implementation and Integrations • Information Security Control Testing and Evaluation • Information Security Awareness and Training/td> • Management of External Services

		(e.g., providers, suppliers, third parties, fourth parties) • Information Security Program Communications and Reporting
Domain 04: (30%) Incident Management	A. Incident Management Readiness	• Incident Response Plan • Business Impact Analysis (BIA) • Business Continuity Plan (BCP) • Disaster Recovery Plan (DRP) • Incident Classification/Categorization • Incident Management Training, Testing, and Evaluation
	B. Incident Management Operations	• 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

Exam Details

Exam Details	**(CISM Exam)**
Number of Questions	**150 Questions; (25% Domain 1 / 30% Domain 2 / 50% Domain 3 / 45% Domain 4)**
Test Duration	**4 Hours**
Test Format	**Multiple Choice**
Test Delivery	**Person VUE (Testing Centers / Online Testing)**
Passing Score	**450 out of 800**