Certified Information Security Manager (CISM)

Gain skill and ability design, implement, assess and manage and enterprise's information security.

Exam and Course Outline

CODEC Networks Pvt Ltd

507, New Delhi House, Barakhamba Road, New Delhi 110001 trainings@codecnetworks.com
+91 11 43752299, 9971676124

Course Overview

Certified Information Security Manager (CISM) is a registered trademark and course developed by ISACA and the most globally recognized certification among information security management professionals craft skills to effective security management and consulting services.

CISM course and certification exam ensure professional's to demonstrate their capabilities in developing and managing information security programs along with understanding the core relationship with overall business goals.

The course is designed purposely to give participants an idea to decide how valuable the CISM is, and understand to attain the certification.

This course is based on guidelines to cover the below following topics / domains and provide participants a curve in there preparation of CISM Exam.

Domain 1 - Information Security Governance
Domain 2 - Information Risk Management
Domain 3 - Information Security Program Development and Management
Domain 4 - Information Security Incident Management

This preparation course focuses and develops understanding needed to efficiently evaluate, improve and direct organizational information security.

By attending this course, professionals will get a comprehensive review to advance and achieve a robust information security posture to encourage the confidence of management in respective organization's information security

Upon successful passing the CISSP Exam, professional will gain the skills and knowledge necessary to:

- Understand the relationship between Information security and business goals along with objectives.
- Learn to develop an information security governance framework.
- Learn to identify, manage and guard an organization's assets for Information security perspective.
- Learn to manage IT risk to an organizationally acceptable level.
- Learn to define and design security architecture for your IT operation.
- Learn to develop and execute the capability to detect, investigate, remediate and recover from security incidents.
- Focus on IT compliance and the integrity of enterprise systems to establish a more secure enterprise IT framework

Who Should Attend

This program is intended for professionals who have at least 5 years of in Information Systems Security auditing, control or work experience. The program is ideal for those working in positions such as, but not limited to -

- IT Auditors / Manager, Security Consultant / Manager, IT Director / Manager, Systems Engineer / Analyst, CIO, CTO, CISO or anyone willing to learn how to manage, design, supervise or evaluate an enterprise's information security.

Course Duration

32 Hours (4 Days * 8 Hours)

Course Content / Outline

Domain 1 – Information Security Governance

- Explain the need for and the desired outcomes of an effective information security strategy
- Create an information security strategy aligned with organizational goals and objectives
- Gain stakeholder support using business cases
- Identify key roles and responsibilities needed to execute an action plan
- Establish metrics to measure and monitor the performance of security governance

Domain 2 – Information Risk Management

- Explain the importance of risk management as a tool to meet business needs and develop a security management program to support these needs
- Identify, rank, and respond to a risk in a way that is appropriate as defined by organizational directives
- Assess the appropriateness and effectiveness of information security controls
- Report information security risk effectively

Domain 3 – Information Security Program Development and Management

- Align information security program requirements with those of other business functions
- Manage the information security program resources
- Design and implement information security controls
- Incorporate information security requirements into contracts, agreements and third-party management processes

Domain 4 – Information Security Incident Management

- Understand the concepts and practices of Incident Management
- Identify the components of an Incident Response Plan and evaluate its effectiveness
- Understand the key concepts of Business Continuity Planning, or BCP and Disaster Recovery Planning, or DRP
- Be familiar with techniques commonly used to test incident response capabilities