Certified Information Security Manager CISM 4 Days

This Certified Information Security Manager (CISM) training course focuses on the construction, development, and governance of information security operations. Possession of this certification displays precise knowledge, practice, and copious amounts of experience in the realm of information security management. This CISM training course takes into account practical issues, like the creation of information security programs, and incident management, whilst promoting security practices used globally. CISM teaches delegates how to tailor ever-changing technology to their enterprises. This enables the enterprises to emerge as a valuable organisation and may expand their clientele due to their implementation of CISM certified individuals.

The demand for skilled information security management professionals is increasing, hence this CISM certification fulfils business needs. CISM has been accepted as the universal standard to strive towards within the sphere of information security, thus depicting the qualification as a prominent representation of expertise and commitment. This causes CISM holders to be identified as the most certified professionals in the information security realm and means delegates can recognise the link between information security programs and the larger goals of the organisation.

The four domains are as follows:

1. Information Security Governance
2. Information Risk Management and Compliance
3. Information Security Program Development and Management
4. Information Security Incident Management

Target Audience

CISM certification is a globally recognised professional requirement in the IT Security domain. This certification is best suited for:

- Security consultants and managers
- IT directors and managers
- Security auditors and architects
- Security systems engineers
- Chief Information Security Officers (CISOs)
- Information security managers
- IS/IT consultants
- Chief Compliance/Privacy/Risk Officers

The above list is a suggestion only; individuals may wish to attend based on their own career aspirations, personal goals or objectives. Delegates may take as few or as many Intermediate qualifications as they require, and to suit their needs.

Delegates wishing to take the official ISACA Certified Information Security Manager (CISM) exam will need to book this directly with ISACA.

Prerequisites

There are no prerequisites to learn CISM from this tutorial. However, to get the CISM certification you need to:

- Pass the CISM examination
- Submit an application for CISM certification
- Adhere to the Code of Professional Ethics
- Dedicate to the Continuing Professional Education Program
- Compliance with the Information Security Standards

The examination is open to all individuals who have an interest in information security. A minimum of 5 years of professional information systems auditing, control or security work experience is required for the CISM certification.

Please note: This exam is sat seperately from the course. Delegates must purchase an exam voucher directly from ISACA.

Learning Outcomes

This CISM course will give you the requisite skillsets to design, deploy and manage security architecture for your organisation. The course is aligned with ISACA best practices and is designed to help you pass the CISM exam on your first attempt. Enterprises and government agencies increasingly expect their IT professionals to hold a CISM certification, and it is considered essential to ongoing education and career development. This course will see that you are well-equipped to manage the ongoing security, compliance and governance of your IT organisation.

Course Outline

This CISM training course covers the following areas:

- Introduction to Certified Information Security Manager (CISM)
- Objectives and Expectations
- What is Information Security?
- The Goals of Information Security
- Principles for Information Security Professionals

Domain 1 – Information Security Governance

- Introduction to Information Security Governance
- Effective Information Security Governance
- Governance and Third Party Relationships
- Information Security Metrics
- Information Security Governance Metrics
- Information Security Strategy
- Information Security Strategy Development
- Strategy Resources and Constraints
- Other Frameworks
- Compliances
- Action Plans to Implement Strategy
- Governance of Enterprise IT

Domain 2 – Information Risk Management and Compliance

- Information Risk Management
- Risk Management Overview
- Risk Assessment
- Information Asset Classification
- Assessment Management
- Information Resource Valuation
- Recovery Time Objectives
- Security Control Baselines
- Risk Monitoring

- Training and Awareness
- Information Risk Management Documentation

Domain 3 – Information Security Program Development and Management

- Information Security Program Management Overview
- Information Security Program Objectives
- Information Security Program Concepts
- Information Security Program Technology Resources
- Information Security Program Development
- Information Security Program Framework
- Information Security Program Roadmap
- Enterprise Information Security Architecture (EISA)
- Security Program Management and Administration
- Security Program Services and Operational Activities
- Controls
- Security Program Metrics and Monitoring
- Measuring Operational Performance
- Common Information Security Program Challenges

Domain 4 – Information Security Incident Management

- Incident Management Overview
- Incident Management Procedures
- Incident Management Resources
- Incident Management Objectives
- Incident Management Metrics and Indicators
- Defining Incident Management Procedures
- Business Continuity and Disaster Recovery Procedures
- Post Incident Activities and Investigation
- ISACA Code of Professional Ethics
- Laws and Regulations
- Policy Versus Law Within an Organisation
- Ethics and the Internet IAB
- Certified Information Security Manager