CISM Certified Information Security Manager
An ISACA® Certification

Course Description

General Information:

Designed for IT professionals with technical expertise and experience in IS/IT security and control looking to transition from team player to manager. CISM can add credibility and confidence to interactions with internal and external stakeholders, peers and regulators.

This certification indicates expertise in information security governance, program development and management, incident management and risk management. If you are a mid-career IT professional aspiring to senior management roles in IT security and control, CISM can get you the visibility you need.

There are 150 Questions on the exam which must be completed in 4 hours. It is available online via remote proctoring and at in-person testing centers where available.

The CISM Certification is intended for:

Information security professionals with at least 5 years of relevant work experience, with at least 3 years in the role of information security manager. Job titles include:

- CISO
- CSO
- Security Director/Manager/Consultant
- IT Director/Manager/Consultant
- Compliance/Risk/Privacy Director and Manager

CPE Overview:

To maintain your CISM, you must earn and report a minimum of 120 CPE hours every 3-year reporting cycle and at least 20 hours annually. CISM awards up to 1 hour of CPE for every 1 hour of instructor led training. Online review course earns 21 CPEs and Virtual Instructor-Led Training (VILT) earns 14 CPEs.

Course Duration:

Online Course: Approximately 17 hours

In-person training or VILT: 2-4 days

Course Topics Include:

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