Course Description

CISM Certified Information Security Manager® An ISACA® Certification

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 four hours. It is available online via remote proctoring and at in-person testing centers where available.

CISM Certification Candidates

CISM is intended for information security professionals with at least five years of relevant work experience and at least three 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 three-year reporting cycle and at least 20 hours annually. CISM awards up to one hour of CPE for every one hour of instructor led training. Online review course earns 20 CPEs and Virtual Instructor-Led Training (VILT) earns 14 CPEs.

Course Duration

- Online Course: Approximately 16 hours
- In-person training or VILT: 2–4 days

Course Topics

Domain 1: Information Security Governance

- Enterprise Governance Overview
- Organizational Culture, Structures, Roles and Responsibilities
- Legal, Regulatory and Contractual Requirements
- Information Security Strategy
- Information Governance Frameworks and Standards
- Strategic Planning

Domain 2: Information Security Risk Management

- Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment, Evaluation and Analysis
- Information Risk Response
- Risk Monitoring, Reporting and Communication

Domain 3: Information Security Program

- IS Program Development and Resources
- IS Standards and Frameworks
- Defining an IS Program Road Map

Domain 3: Information Security Program, continued

- IS Program Metrics
- IS Program Management
- IS Awareness and Training
- Integrating the Security Program with IT Operations
- Program Communications, Reporting and Performance Management

Domain 4: Incident Management

- Incident Management and Incident Response Overview
- Incident Management and Response Plans
- Incident Classification/Categorization
- Incident Management Operations, Tools and Technologies
- Incident Investigation, Evaluation, Containment and Communication
- Incident Eradication, Recovery and Review
- Business Impact and Continuity
- Disaster Recovery Planning
- Training, Testing and Evaluation