Document Generated: 07/10/2026

Learning Style: Virtual Classroom

Technology: ISACA

Difficulty: Intermediate

Course Duration: 3 Days

Next Course Date: September 22, 2026

Certified Information Security Manager (CISM) Exam Preparation

About this course

This course of information security training is specially developed for information security professionals who are getting ready to give the CISM exam. It is getting tougher to secure enterprise data therefore, this information security training ISACA

course helps you give a detailed coverage on the four CISM domains. These domains include, risk management and compliance; security incident management; security governance and security program development and management.

The average salary for Certified Information Security Manager is **$116,155** per year.

Course Objective

After completing this course, students will be able to:

- Create an overall information security design and maintain its operations and working.
- Design the measures to take for strategy execution along with creating an information security strategy.
- React to and recuperate from damaging information security happenings.
- CISM (Certified Information Security Manager) examination preparation and completion.
- Handle and control all sorts of information security threats.

Audience

The course designed for:

- People associated with IT work like IT managers, auditors or consultants.
- Professionals with information security responsibilities like security device administrators, policy writers, officers, information security managers and security engineers.
- Network administrators

Prerequisites

- Five years of information security practice is must for all security engineers and device administrators, IT auditors, professionals, managers, privacy officers, consultants, security policy writers and information security officers.

Suggested prerequisites courses

- Certified Ethical Hacking (CEH)
- Certified Information Systems Security Professional (CISSP)

Course Outline:

Module 1: Information Security Governance

In this module, you will learn how to:

- Establish and maintain an information security strategy and align the strategy with corporate governance
- Identify internal and external influences to the organization
- Define roles and responsibilities
- Establish, monitor, evaluate, and report metrics

Module 2: Information Risk Management and Compliance

In this module, you will learn how to:

- Establish a process for information asset classification and ownership
- Identify legal, regulatory, organizational, and other applicable requirements
- Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted periodically
- Determine appropriate risk treatment options
- Evaluate information security controls
- Identify the gap between current and desired risk levels
- Integrate information risk management into business and IT processes
- Monitor existing risk
- Report noncompliance and other changes in information risk

Module 3: Information Security Program Development and Management

In this module, you will learn how to:

- Establish and maintain the information security program
- Identify, acquire, manage, and define requirements for internal and external resources

- Establish and maintain information security architectures
- Establish, communicate, and maintain organizational information security standards, procedures, and guidelines
- Establish and maintain a program for information security awareness and training
- Integrate information security requirements into organizational processes, as well as into contracts and activities of third parties
- Establish, monitor, and periodically report program management and operational metrics

Module 4: Information Security Incident Management

In this module, you will learn how to:

- Establish and maintain an organizational definition and severity hierarchy for information security incidents
- Establish and maintain an incident response plan
- Develop and implement processes to ensure timely identification of information security incidents
- Establish and maintain processes to investigate and document information security incidents
- Establish and maintain incident escalation and notification processes
- Organize, train, and equip teams to effectively respond to information security incidents
- Test and review the incident response plan periodically
- Establish and maintain communication plans and processes
- Conduct post-incident reviews
- Establish and maintain integration among the incident response plan, disaster recovery plan, and business continuity plan