CISM Certified Information Security Manager

Course 2036

- Duration: **4 days**
- Exam Voucher: **Yes**
- Language: **English**
- Level: **Intermediate**
- **23 NASBA CPE Credits**

In this course, you will gain the knowledge and skills needed to successfully pass the certification exam and become a **CISM Certified Information Security Manager**.

This course will cover four CISM domains:

- Security governance
- Risk management and compliance
- Security program development and management
- Security incident management

In addition to meeting ISACA's certification requirements, passing the CISM Certification Exam meets U.S. DoD Directive 8140/8570.01 Management (IAM) Level-II, Management (IAM) Level-III and CSSP Manager requirements.

CISM Certified Information Security Manager Training Delivery Methods

- In-Person
- Online

CISM Certified Information Security Manager Training Information

In this course, you will:

- Learn from ISACA official curriculum.
- Receive an exam voucher from ISACA.
- Prepare for and pass the Certified Information Security Manager (CISM) exam.
- Develop an information security strategy and plan of action to implement the strategy.
- Manage and monitor information security risks.
- Build and maintain an information security plan.
- Implement policies and procedures to respond to and recover from disruptive and destructive information security events.
- Continue learning and face new challenges with after-course one-on-one instructor coaching.

Training Prerequisites

To succeed in this course and successfully pass the CISM exam, you should have at least five years of information security experience in at least one of the following roles:

- IT consultant, auditor, or manager
- Security policy writer
- Privacy officer
- Information security officer
- Network administrator
- Security device administrator
- Security engineers

Certification Information

The ISACA Exam Candidate Information Guide provides valuable information regarding exam day rules and information, as well as exam dates and deadlines. You can find the most recent version at ISACA.org

CISM Certified Information Security Manager Training 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