

## Certified Information Security Manager® (CISM)

### Overview

---

This course is designed to help candidates prepare for sitting the ISACA CISM certification examination. By taking this course and obtaining CISM certification, your experience and skills in supporting the information security needs of your organization will be validated. Securing the organization's information is a critical business objective in today's business environment. The information that an organization depends on to be successful can be at risk from numerous sources. By effectively managing information security, you can address these risks and ensure the organization remains healthy and competitive in the marketplace.

### Prerequisite Comments

---

To ensure your success, you should have at least five years of professional experience in information security, as well as at least three years of experience in information security management. You are also required to prove this level of experience to ISACA in order to obtain certification. Major areas of information security management include:

- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

### Target Audience

---

The intended audience for this course is information security and IT professionals, particularly IT managers who are interested in earning the CISM certification. The course is also applicable to individuals who are interested in learning in-depth information about information security management or who are looking for career advancement in IT security.

### Course Objectives

---

Upon successful completion of this course, students will be able to:

- establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.
- identify and manage information security risks to achieve business objectives.
- create a program to implement the information security strategy.
- implement an information security program.
- oversee and direct information security activities to execute the information security program.
- plan, develop, and manage capabilities to detect, respond to, and recover from information security incidents.

### Course Outline

---

## 1 - Information Security Governance

- Develop an Information Security Strategy
- Align Information Security Strategy with Corporate Governance
- Identify Legal and Regulatory Requirements
- Justify Investment in Information Security
- Identify Drivers Affecting the Organization
- Obtain Senior Management Commitment to Information Security
- Define Roles and Responsibilities for Information Security
- Establish Reporting and Communication Channels

## 2 - Information Risk Management

- Implement an Information Risk Assessment Process
- Determine Information Asset Classification and Ownership
- Conduct Ongoing Threat and Vulnerability Evaluations
- Conduct Periodic BIAs
- Identify and Evaluate Risk Mitigation Strategies
- Integrate Risk Management into Business Life Cycle Processes
- Report Changes in Information Risk

## 3 - Information Security Program Development

- Develop Plans to Implement an Information Security Strategy
- Security Technologies and Controls
- Specify Information Security Program Activities
- Coordinate Information Security Programs with Business Assurance Functions
- Identify Resources Needed for Information Security Program Implementation
- Develop Information Security Architectures
- Develop Information Security Policies
- Develop Information Security Awareness, Training, and Education Programs
- Develop Supporting Documentation for Information Security Policies

## 4 - Information Security Program Implementation

- Integrate Information Security Requirements into Organizational Processes
- Integrate Information Security Controls into Contracts
- Create Information Security Program Evaluation Metrics

## 5 - Information Security Program Management

- Manage Information Security Program Resources
- Enforce Policy and Standards Compliance
- Enforce Contractual Information Security Controls
- Enforce Information Security During Systems Development
- Maintain Information Security Within an Organization
- Provide Information Security Advice and Guidance
- Provide Information Security Awareness and Training
- Analyze the Effectiveness of Information Security Controls
- Resolve Noncompliance Issues

## 6 - Incident Management and Response

Develop an Information Security Incident Response Plan  
Establish an Escalation Process  
Develop a Communication Process  
Integrate an IRP  
Develop IRTs  
Test an IRP  
Manage Responses to Information Security Incidents  
Perform an Information Security Incident Investigation  
Conduct Post-Incident Reviews

## Related Courses, Certifications, Exams

---

- Certified Information Security Manager® (CISM)
  - CISM - Certified Information Security Manager (CISM)
-