

# Certified Information Security Manager (CISM) Exam Preparation Training Course



## Course Description:

The Certified Information Security Manager (CISM) training course is designed to help you prepare for ISACA's Certified Information Security Manager (CISM) exam. The CISM certification is globally recognized and validates your expertise in information security management.

This training course covers all four domains of the CISM framework in depth, providing you with a solid foundation in information security management principles and practices. By the end of this course, you'll be well-prepared to tackle the CISM exam and advance your career in information security management.

This training course is designed using the exam syllabus and will be delivered by a trainer who has successfully taken and passed the official exam.

**This exam preparatory Certified Information Security Manager (CISM) training course will highlight;**

- Essential concepts and best practices
- Review real-world case studies
- Complete practice questions and mock exams
- Strategies for exam success

## Objectives

This comprehensive CISM exam preparation training course is designed to equip you with the knowledge, skills, and confidence needed to excel in the ISACA Certified Information Security Manager exam.

**At the end of this Certified Information Security Manager (CISM) training course, you will learn to:**

- Master the core concepts and methodologies across all four CISM domains.
- Develop practical skills in implementing and managing information security programs within organizational contexts.
- Enhance critical thinking and problem-solving abilities for addressing complex information security challenges.
- Build proficiency in risk assessment, incident response, and governance frameworks.
- Gain test-taking strategies and experience through practice exams and quizzes to maximize your performance on the CISM certification exam.

### Training Methodology

Through a combination of lectures, interactive discussions, case studies, and hands-on exercises, you'll develop a thorough understanding of how to effectively manage, design, oversee, and assess an enterprise's information security program.

### Organizational Impact

Information security professionals can significantly enhance an organization's information security posture and overall risk management capabilities. By implementing best practices learned through CISM certification, organizations can build robust security programs, improve incident response capabilities, and foster a culture of security awareness. This, in turn, leads to improved operational efficiency, reduced risk exposure, and enhanced stakeholder confidence.

### Impact on the organization:

- Improved alignment of security strategies with business goals, leading to more effective resource allocation and risk management.
- Enhanced ability to identify, assess, and mitigate information security risks, reducing the likelihood and potential impact of security incidents.
- Increased efficiency in security operations through standardized processes and frameworks, resulting in cost savings and improved performance.

- Strengthened compliance posture, helping the organization meet regulatory requirements and industry standards more effectively.
- Better preparedness for and response to security incidents, minimizing potential damages and recovery time.
- Elevated reputation and trust among customers, partners, and stakeholders, potentially leading to competitive advantages and new business opportunities.

### **Personal Impact**

Completing this training course is an important step in an information security professional's career. It opens doors to new career opportunities, higher-level positions, and increased responsibilities within organizations. This training course not only enhances your technical knowledge but also develops your strategic thinking and leadership skills, positioning you as a valuable asset in bridging the gap between IT security and business objectives. This certification can lead to personal growth, professional recognition, and increased job satisfaction.

At the end of this training course, the participants will gain the following;

- Career advancement: Increased potential for promotions and access to senior-level information security management positions.
- Enhanced credibility: Recognition as a trusted advisor in information security matters among peers, executives, and stakeholders.
- Expanded professional network
- Improved skills: Development of a well-rounded skill set that combines technical knowledge with business acumen and strategic thinking.
- Personal satisfaction: Sense of accomplishment and confidence in one's ability to effectively manage information security at an enterprise level

### **WHO SHOULD ATTEND?**

The CISM exam preparation training course is ideal for experienced information security professionals seeking to advance their careers and validate their expertise in information security management.

**This Certified Information Security Manager (CISM) training course is suitable to a wide range of professionals but will greatly benefit:**

- IT Security Managers
- Information Security Consultants and Auditors
- Risk Management Professionals
- IT Governance Specialists
- Aspiring security leaders

## Course Outline:

### **DAY 1**

#### **Enterprise Governance**

- Organizational Culture
- Legal, Regulatory and Contractual Requirements
- Organizational Structures, Roles and Responsibilities

#### **Information Security Strategy**

- Information Security Strategy Development
- Information Governance Frameworks and Standards
- Strategic Planning (e.g., Budgets, Resources, Business Case)

### **DAY 2**

#### **Information Security Risk Assessment**

- Emerging Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment and Analysis

#### **Information Security Risk Response**

- Risk Treatment / Risk Response Options

- Risk and Control Ownership
- Risk Monitoring and Reporting

### **DAY 3**

#### **Information Security Program Development**

- Information Security Program Resources (e.g., People, Tools, Technologies)
- Information Asset Identification and Classification
- Industry Standards and Frameworks for Information Security
- Information Security Policies, Procedures and Guidelines
- Information Security Program Metrics

#### **Information Security Program Management**

- Information Security Control Design and Selection
- Information Security Control Implementation and Integrations
- Information Security Control Testing and Evaluation

### **DAY 4**

#### **Security Awareness**

- Information Security Awareness and Training
- Management of External Services (e.g., Providers, Suppliers, Third Parties, Fourth Parties)
- Information Security Program Communications and Reporting

#### **Incident Management Readiness**

- Incident Response Plan
- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Classification/Categorization



- Incident Management Training, Testing and Evaluation

## **DAY 5**

### **Incident Management Operations**

- Incident Management Tools and Techniques
- Incident Investigation and Evaluation
- Incident Containment Methods
- Incident Response Communications (e.g., Reporting, Notification, Escalation)
- Incident Eradication and Recovery
- Post-Incident Review Practices