Certified Information Security Manager (CISM) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

- **Build the expertise to design, deploy, and manage security architecture confidently across your organisation.**
- **Designed for security managers, CISOs, and professionals who require strong governance and risk management capabilities.**
- **ISACA-aligned training designed to provide comprehensive preparation for the CISM examination.**

The Certified Information Security Manager (CISM) training course focuses on the development, implementation, and governance of information security operations. The CISM certification demonstrates professional knowledge, practical capability, and experience in information security management.

The course goes beyond theoretical security concepts by addressing practical areas such as developing information security programmes, managing organisational risk, and responding to security incidents. Participants learn how evolving technologies and security requirements can be managed in accordance with the needs and objectives of an organisation.

Rather than approaching information security purely as a technical discipline, CISM connects security management with wider organisational goals. This enables security professionals to understand how information security programmes can support business priorities and contribute to effective enterprise governance.

This certification is a **DoD Approved 8570 Baseline Certification** and meets **DoD 8140/8570 training requirements.**

As demand for experienced information security management professionals continues to grow, CISM has become a widely recognised professional certification within the information security field. It is particularly relevant to professionals responsible for security governance, risk management, security programme management, and incident management.

CISM is structured around four domains:

1. **Information Security Governance**
2. **Information Risk Management**
3. **Information Security Program Development and Management**
4. **Information Security Incident Management**

This course includes the official ISACA CISM Exam and the official ISACA Exam Prep Tool.

Prerequisites

There are no mandatory prerequisites for studying the CISM subject matter. However, candidates wishing to obtain the CISM certification must satisfy the certification requirements established by ISACA.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

These requirements include:

- Passing the CISM examination
- Submitting an application for CISM certification
- Paying a $50 application fee directly to ISACA
- Adhering to the ISACA Code of Professional Ethics
- Committing to the Continuing Professional Education (CPE) Programme
- Complying with applicable information security standards

The examination is open to individuals interested in information security. However, a minimum of **five years of professional information systems auditing, control, or security work experience** is required before the CISM certification can be awarded.

Who Should Attend

CISM is a globally recognised professional certification within the IT and information security field. This training is particularly suitable for:

- Security consultants and managers
- IT directors and managers
- Security auditors and architects
- Security systems engineers
- Chief Information Security Officers (CISOs)
- Information security managers
- IS/IT consultants
- Chief Compliance, Privacy, and Risk Officers

The roles above represent a suggested audience rather than a restriction. Professionals may also attend according to their career aspirations, development goals, or organisational responsibilities.

Certified Information Security Manager (CISM) Training

Duration: **4 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

The CISM course is designed to develop the skills required to design, deploy, and manage security architecture and information security programmes within an organisation.

The programme is aligned with ISACA information security management practices and structured to support participants preparing for the CISM examination.

By completing the training, participants will develop their ability to:

- Understand and evaluate information security governance
- Identify, assess, and manage information security risks
- Develop and manage enterprise information security programmes
- Monitor the effectiveness and performance of security programmes
- Establish and manage information security incident processes
- Align security, governance, compliance, and risk activities with organisational objectives

CISM Domain Weightings

The CISM examination is divided across four domains with the following weightings:

Domain	Exam Weight
Domain 1: Information Security Governance	17%
Domain 2: Information Risk Management	20%
Domain 3: Information Security Program Development and Management	33%
Domain 4: Information Security Incident Management	30%
Total	**100%**

Outline

Introduction to CISM

The introductory section establishes the fundamental principles and objectives that support the remainder of the programme.

Topics include:

- Introduction to Certified Information Security Manager (CISM)
- Course objectives and expectations
- What is information security?
- Goals of information security
- Principles for information security professionals

Domain 1 – Information Security Governance

This domain examines how information security should be governed across an organisation and how security strategy can be aligned with enterprise objectives.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Topics include:

- Introduction to information security governance
- Effective information security governance
- Governance and third-party relationships
- Information security metrics
- Information security governance metrics
- Information security strategy
- Developing an information security strategy
- Strategy resources and constraints
- Other frameworks
- Compliance requirements
- Action plans for implementing strategy
- Governance of enterprise IT

Domain 2 – Information Risk Management

This domain covers the practices organisations use to identify, assess, monitor, document, and manage information security risks.

Topics include:

- Information risk management
- Risk management overview
- Risk assessment
- Information asset classification
- Assessment management
- Information resource valuation
- Recovery Time Objectives
- Security control baselines
- Risk monitoring
- Training and awareness
- Information risk management documentation

Domain 3 – Information Security Program Development and Management

This domain focuses on the development, implementation, administration, and continuous management of enterprise information security programmes.

Topics include:

- Information security programme management overview
- Information security programme objectives
- Information security programme concepts
- Technology resources for information security programmes
- Information security programme development
- Information security programme frameworks
- Information security programme roadmaps
- Enterprise Information Security Architecture (EISA)
- Security programme management and administration
- Security programme services and operational activities
- Controls

- Security programme metrics and monitoring
- Measuring operational performance
- Common information security programme challenges

Domain 4 – Information Security Incident Management

This domain addresses the processes and resources required to prepare for, respond to, recover from, and review information security incidents.

Topics include:

- Incident management overview
- Incident management procedures
- Incident management resources
- Incident management objectives
- Incident management metrics and indicators
- Defining incident management procedures
- Business continuity and disaster recovery procedures
- Post-incident activities and investigation

Ethics, Regulations, and Professional Responsibilities

The course also addresses professional, ethical, and regulatory considerations relevant to information security managers.

Topics include:

- ISACA Code of Professional Ethics
- Laws and regulations
- Organisational policy versus law
- Ethics and the Internet
- Certified Information Security Manager professional responsibilities

ISACA Product Access Period Changes

Important Update Effective 16 April 2026

Effective **16 April 2026**, ISACA is reducing product access periods from **12 months to 6 months** across a range of products, including Exams, QAE, Online Review Courses, non-sponsored Webinars, and Virtual Workshops.

How the New Access Windows Work

1. Assignment and Redemption Window

Products must be assigned and redeemed within **six months of the purchase date**.

2. Access and Completion Window

Once a product has been redeemed, learners receive **six months of access** to use it. Depending on the

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

relevant product, this period includes:

- Accessing learning content
- Scheduling examinations
- Sitting examinations

What This Means for Learners

Review Manuals: Learners continue to receive long-term access.

QAE Databases & Online Review Courses: Available for six months following redemption.

Exams: Must be scheduled and completed within six months of redemption.

Learners are encouraged to redeem their products promptly and plan their study and examination schedules early to make effective use of the available access period.

Exams and Assessments

The course fee includes the **official ISACA CISM Exam** and the **official ISACA Exam Prep Tool**.

To achieve the CISM certification, candidates must successfully complete the examination and submit a certification application to ISACA. They must also pay the $50 application fee directly to ISACA, adhere to the ISACA Code of Professional Ethics, and commit to the Continuing Professional Education (CPE) Programme.

A minimum of **five years of professional information systems auditing, control, or security work experience** is required before the CISM certification can be awarded.

Under ISACA's updated product access policy effective **16 April 2026**, learners have **six months following redemption** to access applicable learning content, schedule their examination, and sit the exam. Candidates are therefore encouraged to redeem their products promptly and plan their study and examination schedule accordingly.