Certified Information Systems Auditor (CISA) Training

Duration: **4 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Overview

- **Develop the skills to audit, control, assess, and secure information systems across all five ISACA domains.**
- **Designed for experienced IS auditors, compliance professionals, and other specialists preparing for the CISA credential.**
- **Expert-led training aligned with the updated 2024 CISA Exam Content Outline.**

Certified Information Systems Auditor (CISA) is a globally recognised certification for professionals working in information systems auditing, control, and security. It builds on existing professional experience and develops the knowledge required to assess information systems, organisational controls, governance practices, and security processes effectively.

CISA is recognised as a **DoD Approved 8570 Baseline Certification** and meets **DoD 8140/8570 training requirements.**

Throughout this CISA training course, participants explore the five core domains that form the foundation of the CISA examination and certification framework. Each domain addresses a different area of information systems auditing, governance, development, operations, and information asset protection.

The programme covers a substantial amount of material and is therefore considered intensive. Participants are encouraged to review the subjects covered during the training and dedicate sufficient individual study time to their CISA exam preparation.

The five CISA domains are:

1. **Information Systems Auditing Process**
2. **Governance and Management of IT**
3. **Information Systems Acquisition, Development, and Implementation**
4. **Information Systems Operations and Business Resilience**
5. **Protection of Information Assets**

Prerequisites

There are no mandatory prerequisites for learning the CISA subject matter. However, candidates who wish to obtain the CISA certification must satisfy the certification requirements established by ISACA.

These include:

- Passing the CISA examination
- Submitting an application for CISA certification
- Paying a $50 certification application fee directly to ISACA
- Adhering to the ISACA Code of Professional Ethics
- Committing to the Continuing Professional Education (CPE) Programme

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Complying with Information Systems Auditing Standards

The CISA examination is open to individuals interested in information systems auditing, control, and security. However, obtaining the CISA certification requires a minimum of **five years of professional experience** in information systems auditing, control, or security.

Because of the depth and intensity of the programme, this training is particularly suitable for professionals who already have significant exposure to information systems auditing. CISA can provide an important professional credential for individuals seeking to progress in auditing, governance, risk, security, and compliance roles.

Who Should Attend

CISA training is intended for professionals responsible for controlling, monitoring, assessing, or auditing an organisation's information technology and business systems.

Typical participants include:

- IS/IT auditors and consultants
- IT compliance managers
- Chief Compliance Officers
- Chief risk and privacy officers
- Information security heads and directors
- Security managers and architects

This list is provided as guidance rather than a restriction. Professionals may also attend according to their individual career plans, development objectives, or organisational responsibilities.

What You Will Learn

The programme is designed to build participants' understanding across all five CISA domains:

- Information Systems Auditing Process
- Governance and Management of IT
- Information Systems Acquisition, Development, and Implementation
- Information Systems Operations and Business Resilience
- Protection of Information Assets

Outline

Domain 1: Information Systems Auditing Process

This domain focuses on the principles and practices involved in planning and conducting information systems audits.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Key topics include:

- Developing a risk-based IT audit strategy
- Planning individual audit engagements
- Conducting audits in accordance with IS audit standards
- Implementing risk management and control practices

Domain 2: Governance and Management of IT

This domain examines how organisations establish, manage, and evaluate effective IT governance.

Key topics include:

- Assessing the effectiveness of IT governance structures
- IT organisational structures and human resource management
- Organisational IT policies, standards, and procedures
- Evaluating the adequacy of the Quality Management System
- IT management and monitoring controls
- IT resource investments
- IT contracting strategies and policies
- Management of organisational IT-related risks
- Monitoring and assurance practices
- Organisational business continuity planning

Domain 3: Information Systems Acquisition, Development, and Implementation

This domain addresses the controls and management practices associated with information systems throughout acquisition, development, implementation, maintenance, and retirement.

Key topics include:

- Developing business cases for IS acquisition, development, maintenance, and retirement
- Project management practices and controls
- Reviewing project management practices
- Controls covering requirements, acquisition, development, and testing
- Assessing information system readiness
- Reviewing project plans
- Conducting post-implementation system reviews

Domain 4: Information Systems Operations and Business Resilience

This domain focuses on the effective operation, maintenance, availability, and resilience of information systems.

Key topics include:

- Conducting periodic reviews of organisational objectives
- Service level management
- Third-party management practices
- Operational and end-user procedures
- Information systems maintenance processes
- Data administration practices supporting database integrity and optimisation
- Capacity and performance monitoring tools and techniques

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Problem and incident management practices
- Change, configuration, and release management
- Evaluating backup and restoration arrangements
- Assessing organisational disaster recovery plans

Domain 5: Protection of Information Assets

This domain examines the controls and procedures organisations use to protect information and associated assets.

Key topics include:

- Information security policies, standards, and procedures
- Designing, implementing, and monitoring system and logical security controls
- Designing, implementing, and monitoring data classification processes and procedures
- Designing, implementing, and monitoring physical access and environmental controls
- Processes for storing, retrieving, transporting, and securely disposing of information assets

2024 CISA Exam Content and Domain Weightings

The updated CISA Exam Content Outline (ECO) became effective on**1 August 2024**. While the five-domain structure remains in place, the weighting assigned to several domains has changed.

Domain	2019 ECO	2024 ECO
Domain 1: Information Systems Auditing Process	21%	18%
Domain 2: Governance and Management of IT	17%	18%
Domain 3: Information Systems Acquisition, Development, and Implementation	12%	12%
Domain 4: Information Systems Operations and Business Resilience	23%	26%
Domain 5: Protection of Information Assets	27%	26%
Total	**100%**	**100%**

ISACA Product Access Period Changes

Update Effective 16 April 2026

Effective **16 April 2026**, ISACA is changing access periods for a range of products from 12 months to**6 months**. The change applies to Exams, QAE products, 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 original purchase date.

2. Access and Completion Window

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

After redemption, learners receive six months of access to the relevant product. Depending on the product, this period includes accessing learning materials, scheduling examinations, and sitting examinations.

What Does This Mean 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 carefully to make effective use of the available access period.

CISA Exams and Assessments

This course includes the CISA examination, which is delivered by ISACA.

The examination is organised around five domains, with the current domain weightings based on the updated Exam Content Outline that became effective in August 2024.

Under ISACA's updated product access policy, effective April 2026, examination access must be scheduled and the examination completed within **six months of redemption**.

Passing the examination is one part of achieving CISA certification. Candidates must also submit a certification application to ISACA, pay the $50 application fee, follow the ISACA Code of Professional Ethics, participate in the Continuing Professional Education Programme, and comply with Information Systems Auditing Standards.

Candidates must also meet the requirement for at least**five years of professional experience in information systems auditing, control, or security** before obtaining the CISA certification.