

CISA

Certified Information Systems Auditor Training & Certification



Course Highlights



40-Hours LIVE Instructor-Led Training



ISACA Premium Training Partner



Hands-On Audit Evidence, Analytics & Sampling



Accelerate Exam Prep with Flashcards and Mind Maps



Audit IT Assets, Changes & Incidents



Manage Continuity, Recovery & Operational Resilience



Assess Vendors, Performance & Quality Practices



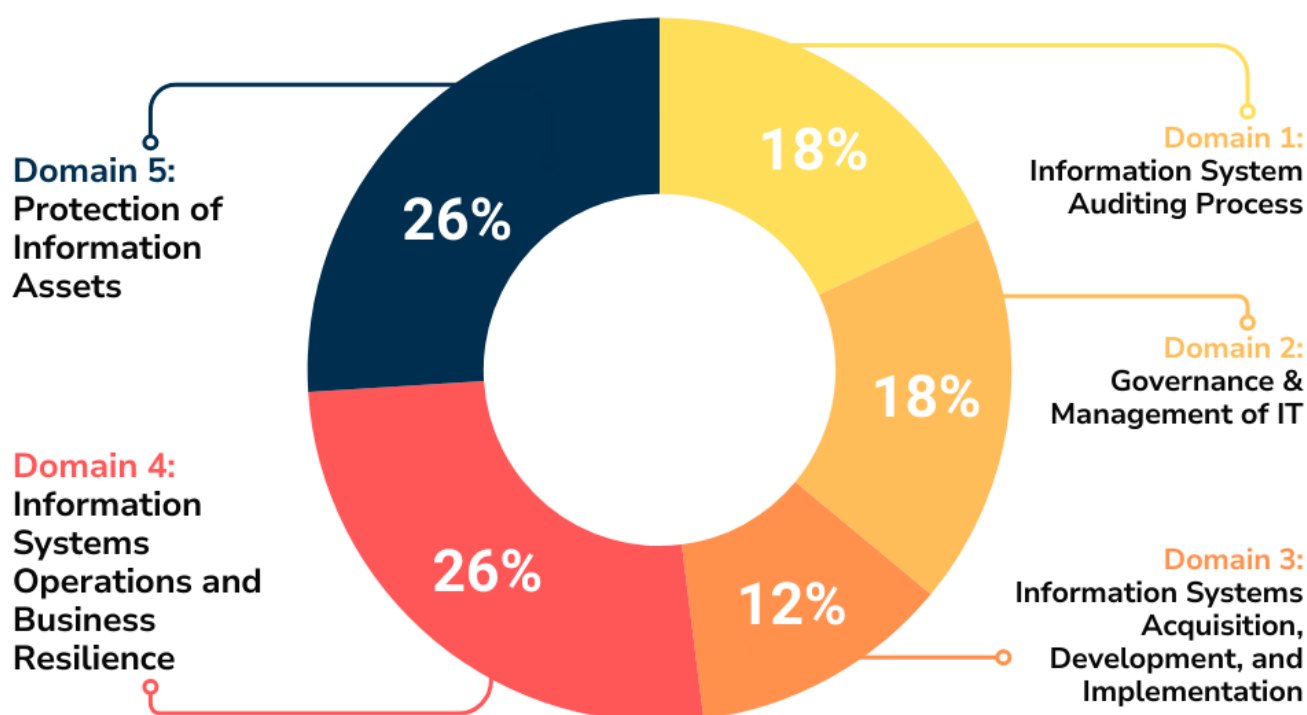
Post Training Support Till Exam



Access to Recorded Sessions

About Course

The CISA certification training course is a globally acknowledged program that prepares IT professionals for excellence in IS auditing, control, and security. Encompassing essential domains such as the Auditing Process, IT Governance and Management, IS Acquisition and Implementation, and Operations and Business Resilience, it culminates with a focus on protecting information assets. This CISA latest version course empowers professionals to assess system vulnerabilities, report compliance, and implement controls, making them vital assets in maintaining organizational integrity and security. Covering the latest 28th edition of CISA, this course addresses all CISA exam changes, ensuring participants are well-prepared for the CISA exam.



Course Objectives

At the end of the course, you will be able to:

- ✔ Plan and execute IS audits using risk-based methodologies, sampling techniques, and evidence collection
- ✔ Apply data analytics and quality assurance practices to strengthen audit reporting and communication
- ✔ Evaluate IT governance frameworks, enterprise architecture, and organizational IT strategy alignment
- ✔ Assess IT vendor management, performance monitoring, and quality management practices
- ✔ Analyze system development methodologies, project governance, and post-implementation review processes
- ✔ Manage IT asset management, change management, patch management, and operational log management
- ✔ Develop and maintain Business Continuity, Disaster Recovery, and Operational Resilience programs
- ✔ Implement Identity and Access Management, Data Encryption, and Network Security controls
- ✔ Conduct Security Incident Response, Evidence Collection, and Forensics investigations
- ✔ Assess Cloud, Virtualized, Mobile, and IoT environments for information asset security risks

Target Audience

- ✓ Individuals who are willing to learn about IS auditing
- ✓ Professionals who are auditors or working in an audit environment
- ✓ Professionals who are willing to make a career in information systems auditing
- ✓ IT Managers
- ✓ Security Managers
- ✓ System Analysts
- ✓ Consultants

Pre-requisites

A minimum of 5 years of professional information systems auditing, control, or security work experience (as described in the CISA job practice areas) is required for certification. Substitutions and waivers of such experience, to a maximum of 3 years, may be obtained as follows:

- ✓ A maximum of 1 year of information systems experience or 1 year of non-information security auditing experience can be substituted for 1 year of experience.
- ✓ 60 to 120 completed university semester credit hours (the equivalent of a 2-year or 4-year degree) not limited by the 10-year preceding restriction can be substituted for 1 or 2 years, respectively, of experience.
- ✓ A master's degree in information security or information technology from an accredited university can be substituted for 1 year of experience.

Exam Information

Exam Name	CISA
Exam Duration	4 Hours
Number of Questions	150
Exam Format	Multiple Choice Questions
Passing Score	450 out of 800
Exam Language	English, French, German, Hebrew, Italian, Japanese, Korean, Spanish, Turkish, Chinese

Course Content

Domain 1

Information System Auditing Process

18%



A-Planning

- ✓ IS Audit Standards, Guidelines, and Codes of Ethics
- ✓ Business Processes
- ✓ Types of Controls
- ✓ Risk-Based Audit Planning
- ✓ Types of Audits and Assessments



B-Execution

- ✓ Audit Project Management
- ✓ Sampling Methodology
- ✓ Audit Evidence Collection Techniques
- ✓ Data Analytics
- ✓ Reporting and Communication Techniques
- ✓ Quality Assurance and Improvement of the Audit Process

Domain 2

Governance and Management of IT

18%



A-IT Governance

- ✓ Laws, Regulations, and Industry Standards
- ✓ Organizational Structure, IT Governance, and IT Strategy
- ✓ IT Policies, Standards, Procedures, and Practices
- ✓ Enterprise Architecture and Considerations
- ✓ Enterprise Risk Management



- ✓ Privacy Program and Principles

- ✓ Data Governance and Classification

B-IT Management

- ✓ IT Resource Management
- ✓ IT Vendor Management
- ✓ IT Performance Monitoring and Reporting
- ✓ Quality Assurance and Quality Management of IT

Domain 3

Information Systems Acquisition, Development, and Implementation | 12%

- ✓ **Information Systems Acquisition and Development**
 - ✓ Project Governance and Management
 - ✓ Business Case and Feasibility Analysis
 - ✓ System Development Methodologies
 - ✓ Control Identification and Design
- ✓ **Information Systems Implementation**
 - ✓ System Readiness and Implementation Testing
 - ✓ Implementation, Configuration, and Release Management
 - ✓ System Migration, Infrastructure Deployment, & Data Conversion
 - ✓ Post-implementation Review

Domain 4

Information Systems Operations and Business Resilience

26%



Information Systems Operations

- ✓ IT Components
- ✓ IT Asset Management
- ✓ Job Scheduling and Production Process Automation
- ✓ System Interfaces
- ✓ Shadow IT and End-User Computing
- ✓ Systems Availability and Capacity Management
- ✓ Problem and Incident Management
- ✓ IT Change, Configuration, and Patch Management
- ✓ Operational Log Management
- ✓ IT Service Level Management
- ✓ Database Management



Business Resilience

- ✓ Business Impact Analysis
- ✓ System and Operational Resilience
- ✓ Data Backup, Storage, and Restoration
- ✓ Business Continuity Plan
- ✓ Disaster Recovery Plans

Domain 5

Protection of Information Assets | 26%

- ✓ **Information Asset Security and Controls**
 - ✓ Information Asset Security Frameworks, Standards, and Guidelines
 - ✓ Physical and Environmental Controls
 - ✓ Identity and Access Management
 - ✓ Network and End-Point Security
 - ✓ Data Loss Prevention
 - ✓ Data Encryption
 - ✓ Public Key Infrastructure
 - ✓ Cloud and Virtualized Environments
 - ✓ Mobile, Wireless, and Internet-of-Things Devices
- ✓ **Security Event Management**
 - ✓ Security Awareness Training and Programs
 - ✓ Information System Attack Methods and Techniques
 - ✓ Security Testing Tools and Techniques
 - ✓ Security Monitoring Tools and Techniques
 - ✓ Security Incident Response Management
 - ✓ Evidence Collection and Forensics



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

