Certified Information Systems Auditor (CISA)

Duration: 5 Days

Method: Instructor-Led Training (ILT) | Live Online Training

***Certification:** Certified Information Systems Auditor (CISA)* —
***Exam:** Certified Information Systems Auditor (CISA)*

Course Description

This exam preparation course is designed to prepare participants for the certification exam. The course focuses on the key points covered in the CISA Review Manual 26th Edition and includes class lectures, group discussions, exam practice and answer debrief.

The CISA designation is a globally recognized certification for IS audit control, assurance, and security professionals. Being CISA certified showcases participants’ audit experience, skills, and knowledge, and demonstrates they are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.

Target Audience

This course is intended for:

- Individuals who audit, control, monitor and assess information technology and business system such as:
  - Information Systems Security Professionals
  - Internal Review Auditors
  - Other Professionals who have an interest in aspects of information systems audit, controls, and security.

Prerequisites

To attend this course, candidates must have:

- met the following requirements as determined by ISACA:
  - Successfully pass the CISA examination.
  - Demonstrate the required minimum (**Five (5) or more years**) work experience in Information Systems auditing, control, assurance, or security
    ***NOTE**: Waivers can be obtained for a maximum of three (3) years. Conditions apply.*
  - Adhere to the Code of Professional Ethics
  - Adhere to the Continuing Professional Education (CPE) Policy:
  - Comply with the Information Systems Auditing Standards:

Exam Details

Exam Code:	• CISA
Length of Exam:	• 4 Hours
Number of Questions:	• 150
Passing Score:	• 450 out of 800 points
Question Format:	• Multiple Choice & Advanced Innovative

Course Objectives

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

- Understand the format and structure of the CISA certification exam.
- Understand the various topics and technical areas covered by the exam.
- Practice specific strategies, tips, and techniques for taking and passing the exam.

Course Topics

Module 1: The Process of Auditing Information Systems

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
- Conduct an audit per IS audit standards and a risk-based IS audit strategy.
- Communicate audit progress, findings, results, and recommendations to stakeholders.
- Conduct audit follow-up to evaluate whether the risk has been sufficiently addressed.
- Evaluate IT management and monitoring of controls.
- Utilize data analytics tools to streamline audit processes.
- Provide consulting services and guidance to the organization to improve the quality and control of information systems.
- Identify opportunities for process improvement in the organization's IT policies and practices.

Course Topics *Continued*

Module 2: Governance and Management of IT

- Evaluate the IT strategy for alignment with the organization's strategies and objectives.
- Evaluate the effectiveness of IT governance structure and IT organizational structure.
- Evaluate the organization's management of IT policies and practices.
- Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements.
- Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives.
- Evaluate the organization's risk management policies and practices.
- Evaluate IT management and monitoring of controls.
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
- Evaluate whether IT supplier selection and contract management processes align with business requirements.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.
- Evaluate data governance policies and practices.
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

Module 3: Information Systems Acquisition, Development, and Implementation

- Evaluate whether the business case for proposed changes to information systems meet business objectives.
- Evaluate the organization's project management policies and practices.
- Evaluate controls at all stages of the information systems development life cycle.
- Evaluate the readiness of information systems for implementation and migration into production.
- Conduct post-implementation review of systems to determine whether project deliverables, controls and requirements are met.
- Evaluate change, configuration, release, and patch management policies and practices.

Course Topics *Continued*

Module 4: Information Systems Operations, Maintenance and Service Management

- Evaluate the organization's ability to continue business operations.
- Evaluate whether IT service management practices align with business requirements.
- Conduct periodic review of information systems and enterprise architecture.
- Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives.
- Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives.
- Evaluate database management practices.
- Evaluate data governance policies and practices.
- Evaluate problem and incident management policies and practices.
- Evaluate change, configuration, release, and patch management policies and practices.
- Evaluate end-user computing to determine whether the processes are effectively controlled.

Module 5: Protection of Information Assets

- Conduct audit per IS audit standards and a risk-based IS audit strategy.
- Evaluate problem and incident management policies and practices.
- Evaluate the organization's information security and privacy policies and practices.
- Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.
- Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.
- Evaluate data classification practices for alignment with the organization's policies and applicable external requirements.
- Evaluate policies and practices related to asset life cycle management.
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.
- Perform technical security testing to identify potential threats and vulnerabilities.
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.

EXERCISES INCLUDED