

CISA TRAINING

EXAM PREPARATION TRAINING

WISELEARNER

WHAT IS CISA?

- The CISA Online Review Course is an online preparation course that prepares learners to pass the CISA certification exam using proven instructional design techniques and interactive activities. The course covers all five of the CISA domains, and each section corresponding directly to the CISA job practice.
- The course incorporates narrated interactive eLearning modules, downloadable job aids, a pre-assessment and practice exam. Learners will be able to navigate the course at their own pace, following a recommended structure, or target preferred job practice areas. Learners may also start and stop the course based on their study schedule, picking up exactly where they left off the next time they access the course.

BENEFIT OF CISA

- CISA is in increasing demand as business analytics, audit control and security are becoming more prevalent and need people with the qualifications that come along with the CISA certification. This credential was once looked at as a "good to have" qualification for job applicants, and now it is preferred in many job requirements for audit control positions. According to Ana Virginia Escalante, CISA, CGEIT, Vice President, SIIAS, SA, "The benefit—the main benefit of the CISA certification in my case-has been to be recognized, not only locally in my country, but at an international level, as a professional with knowledge and skills, able to give an opinion and to audit all the areas related to IT."
- Enhancing your skills
- Increasing the chance of promotion
- Becoming more comfortable with your abilities
- Gain a globally recognised certification



WHO SHOULD ATTEND?

- Professionals preparing to become CISA certified
- Financial auditors moving into IT audit
- IT generalists moving into IT audit
- Mid-level career change
- Students or recent graduates

LEARNING OBJECTIVES

By the end of this course, you will:

- Gain a better understanding of IS audit and assurance guidelines and standards.
- Develop a working knowledge of the five domains of CISA.
- Gives a better understanding of information security audit process
- Gives better awareness of how to protect information systems
- Confirms commitment to profession
- Offers a career differentiator, with enhanced credibility and marketability
- Provides access to valuable resources, such as peer networking and idea exchange



COURSE CONTENTS

Domain 1 — Information System Auditing Process

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
- Conduct an audit in accordance with 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 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 in order to improve the quality and control of information systems.
- Identify opportunities for process improvement in the organization's IT policies and practices.

Domain 2 – Governance & 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

Domain 3 – Information Systems Acquisition, Development, & 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.

Domain 4 – Information Systems Operations and Business Resilience

- 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.

Domain 5 – Protection of Information Assets

- Conduct audit in accordance with 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.



CERTIFICATION

CISA Exam Information:

- Online course
- Downloadable job aids
- Online self-assessment (50 questions)
- Online practice exam (75 questions)

PREREQUISITE

- Submit the complete application within 5 years from the date of initially passing the examination
- Get all the experience you've listed verified by your employers

The experience that you've listed out should have been gained within the 10-year period preceding the date of application, or within five years of passing the examination.

ISACA requires strict professional and academic criteria for candidates wishing to apply for the CISAcertification.

The professional criteria require candidates to have a minimum 4000 actual hours of work experience in full time positions in information systems, security experience and controls. However, candidates can substitute a maximum of 1 year auditing, security and control experience with one year full time experience in information systems or auditing. For university instructors, one year of the required auditing, security and control experience might also be substituted with two years of full educator experience.

Educational Experience Waivers

ACCA (Association of Chartered Certified Accountant) Member recognition

CIMA (Chartered Institute of Management Accountants) full certification

Masters in information technology or information security from a recognized university

WISELEARNER