+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 04/11/2024

Sign up

# CISA© Certification Preparation Course

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

## Presentation

Become a certified IT auditor with our CISA© (Certified Information Systems Auditor) training. We'll teach you everything you need to know to be fully prepared for the exam.

We'll come back to the five main concepts assessed. Firstly, the information system audit process, an essential chapter in carrying out reliable end-to-end audits. Next, we look at IT management and governance.

A section where you will learn how to define and monitor key indicators to ensure compliance with security policies. The acquisition, development and implementation of information systems will show you how to reinforce the clarity of information at all stages of the IT lifecycle.

Then, in the field of resilience, you'll discover how to assess the sustainability of an organization by analyzing its data and IT operations. Finally, you'll strengthen your skills in protecting IT assets through a variety of methods.

## Objectives

- Acquire the knowledge needed to pass the CISA© exam
- Mastering the skills of an IT system auditor
- Know the procedures required to protect IT assets

## Target audience

- ISD
- CISO
- Computer scientist
- Business continuity manager
- Engineer
- Auditor
- Cybersecurity Consultant

# Prerequisites

At least 5 years' experience in IS / IT audit, control, assurance or security. Note: Ambient

IT is not the owner of CISA©, this certification belongs to ISACA©.

# CISA© Certification Preparation Program

## Area 1 - Information systems audit process

- Plan an audit to determine whether information systems are protected and controlled, and whether they add value to the organization.
- Carry out an audit in line with information systems audit standards and strategy risk-based auditing of information systems
- Communicate audit status, findings, results and recommendations to stakeholders
- Follow-up the audit to assess whether risks have been adequately addressed
- Evaluate IT management and control monitoring
- Use data analysis 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 process improvement opportunities in policies and practices organization's IT

## Area 2 - Governance and management of information technologies

- Assess the alignment of IT strategy with the organization's strategies and objectives
- Evaluate the effectiveness of the IT governance structure and the IT organizational structure
- Evaluate the management of the organization's IT policies and practices
- Assess the compliance of the organization's IT policies and practices with legal and regulatory requirements
- Evaluate the management of IT resources and portfolios with a view to aligning them 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 the selection and contractualization of IT suppliers
- Evaluate whether IT supplier selection and contract management processes comply with corporate requirements

- Determine whether IT service management practices comply with business requirements
- 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 the opportunities and potential threats associated with emerging technologies regulations and industry practices

## Area 3 - Acquisition, development and implementation of information systems

- Assess whether the business case for proposed information system changes meets corporate objectives
- Evaluate the organization's project management policies and practices
- Evaluate controls at all stages of the information systems development cycle
- Assess the readiness of information systems for implementation and migration to production.
- Carry out a post-implementation examination of the systems to determine whether the products deliverables, controls and project requirements were met
- Evaluate change, configuration, release and patch management policies and practices

## Area 4 - Information systems operation and business resilience

- Assess the organization's ability to continue as a going concern
- Assess whether IT service management practices comply with corporate requirements
- Carry out a periodic review of the company's information systems and architecture
- Evaluate IT operations to determine whether they are effectively controlled and continue to support the organization's objectives
- Evaluate IT maintenance practices to determine whether they are controlled and if they 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 IT to determine whether processes are adequately controlled. efficient way

## Area 5 - Protecting IT assets

- Perform the audit in accordance with information systems audit standards and a risk-based information systems 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 protected
- Evaluate logical security controls to verify confidentiality, integrity and availability information
- Evaluate data classification practices to ensure compliance with organizational policies and applicable external requirements
- Evaluate asset lifecycle management policies and practices
- Evaluate the information security program to determine its effectiveness and compliance with the organization's strategies and objectives.
- Perform technical security tests to identify threats and vulnerabilities potential
- Assess potential opportunities and threats related to emerging technologies, regulations and industry practices

### Strategies and tips for exam success Mock exam

## Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

## Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

## Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

## Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

## Sanction

A certificate will be issued to each trainee who completes the course.