Certified Information Systems Auditor

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **4 Day**

Overview

Certified Information Systems Auditor (CISA) is a globally acknowledged certification, which builds upon the previous experience of IS professionals, to produce valuable employees who possess exceptional knowledge of Information Systems Auditing, Control, and Security.

During this CISA training course, delegates will be exposed to the Five Domains of Information Security Auditing. These domains comprise the foundations of CISA and it is imperative that delegates grasp a complete understanding of these aspects in order to pass the CISA exam and use their certification within the workplace. Within each of these domains exists multiple topics, which when combined, provide a comprehensive overview of the domain of focus. Due to the breadth of information imparted with each topic over a period of just four days, this course is considered intensive and candidates must study hard to obtain the certification.

The five domains are as follows:

1. The Process of Auditing Information Systems
2. Governance & Management of IT
3. Information Systems Acquisition, Development, and Implementation
4. Information Systems Operations, Maintenance, and Support
5. Protection of Information Assets

The CISA essential for professionals dealing with controlling, monitoring, and assessing an organisation's information technology and business systems. This includes:

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

The above list is a suggestion only; individuals may wish to attend based on their own career aspirations, personal goals or objectives. Delegates may take as few or as many Intermediate qualifications as they require, and to suit their needs.

Delegates wishing to take the official ISACA Certified Information Systems Auditor (CISA) exam will need to book this directly with ISACA.

Prerequisites

There are no prerequisites to learn CISA from this tutorial. However, to get the CISA certification you need to:

- Pass the CISA examination
- Submit an application for CISA certification
- Adhere to the Code of Professional Ethics
- Dedicate to the Continuing Professional Education Program
- Compliance with the Information Systems Auditing Standards

The examination is open to all individuals who have an interest in information systems audit, control, and security. A minimum of 5 years of professional information systems auditing, control or security work experience is required for the CISA certification.

This {*training} is not suitable for beginners. It is required that delegates possess at least five years of exposure in the field of Information Systems Auditing. With this information in mind, it is expected that CISA qualified candidates have an outstanding level of professional experience, commitment, and extensive knowledge of IS Auditing. Thus, a CISA qualification is likely to open many doors and propel certified individuals into a high ranking position within the enterprise.

Please note: This exam is sat seperately from the course. Delegates must purchase an exam voucher directly from ISACA.

What You Will Learn

The five domains within the {*training} are as follows:

- The Process of Auditing Information Systems
- Governance & Management of IT
- Information Systems Acquisition, Development, and Implementation
- Information Systems Operations, Maintenance, and Support
- Protection of Information Assets

Outline

The {*training} content surrounds the pivotal Five Domains. The information imparted within each domain is as follows:

Domain 1: Information Systems Audit Process:

- Developing a risk-based IT audit strategy
- Planning specific audits
- Conducting audits to IS audit standards
- Implementation of risk management and control practices

Domain 2: IT Governance and Management:

- Effectiveness of IT Governance structure
- IT organisational structure and human resources (personnel) management
- Organisation's IT policies, standards, and procedures
- Adequacy of the Quality Management System
- IT management and monitoring controls
- IT resource investment
- IT contracting strategies and policies
- Management of organisations IT-related risks
- Monitoring and assurance practices
- Organisation business continuity plan

Domain 3: Information Systems Acquisition, Development, and Implementation:

- Business case development for IS acquisition, development, maintenance, and retirement
- Project management practices and controls
- Conducting reviews of project management practices
- Controls for requirements, acquisition, development, and testing phases
- Readiness for Information Systems
- Project Plan Reviewing
- Post Implementation System Reviews

Domain 4: Information Systems Operations, Maintenance, and Support:

- Conduct periodic reviews of organisations objectives
- Service level management
- Third party management practices
- Operations and end-user procedures
- Process of information systems maintenance
- Data administration practices determine the integrity and optimisation of databases
- Use of capacity and performance monitoring tools and techniques
- Problem and incident management practices
- Change, configuration, and release management practices
- Adequacy of backup and restore provisions
- Organisation's disaster recovery plan in the event of a disaster

Domain 5: Protection of Information Assets:

- Information security policies, standards and procedures
- Design, implementing, monitoring of system and logical security controls
- Design, implementing, monitoring of data classification processes and procedures
- Design, implementing, monitoring of physical access and environmental controls

- Processes and procedures to store, retrieve, transport and dispose of information assets