Course Outline

CISA - Certified Information Systems Auditor Training Course - 4 days

OVERVIEW

This four-day CISA course is run by the official UK reseller of ISACA's CISA materials and is the perfect intensive preparation course for the CISA exam.

The CISA exam changes every year and our up-to-date course always reflects the latest official guidance on content and exam questions.

The CISA certification demonstrates proficiency in information systems audit and is highly sought after by both professionals and employers alike. Gaining this internationally-recognised qualification will increase recognition in the marketplace and build your influence in the workplace. This Certified Information Systems Auditor (CISA) training course will prepare you to undertake ISACA's challenging CISA exam and is designed to equip you with the knowledge required to achieve a first-time pass.

WHO SHOULD ATTEND THIS CISA TRAINING COURSE?

- Internal and external auditors.
- Finance/CPA professionals.
- IT professionals.
- Information security professionals.

WHAT WILL YOU LEARN?

The training programme mirrors the examination structure and covers the five CISA domains:
- Domain 1: The Process of Auditing Information Systems.
- Domain 2: Governance and Management of IT.
- Domain 3: Information Systems Acquisition, Development, and Implementation.
- Domain 4: Information Systems Operations, Maintenance and Support.
- Domain 5: Protection of Information Assets.

Domain 1: The Process of Auditing Information Systems
- IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards.
- Risk assessment concepts, tools and techniques in an audit context.
- Control objectives and controls related to information systems.
- Audit planning and audit project management techniques, including follow-up.
- Fundamental business processes, including relevant IT.
- Applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits.
- Evidence collection techniques used to gather, protect and preserve audit evidence.
- Sampling methodologies.
- Reporting and communication techniques.
- Audit quality assurance systems and frameworks.

Domain 2: Governance and Management of IT
- IT governance, management, security and control frameworks, and related standards, guidelines, and practices.
- The purpose of IT strategy, policies, standards and procedures for an organisation and the

essential elements of each.
- Organisational structure, roles and responsibilities related to IT.
- Processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures.
- Organisation’s technology direction and IT architecture and their implications for setting long-term strategic directions.
- Relevant laws, regulations and industry standards affecting the organisation.
- Quality management systems.
- Maturity models.
- Process optimization techniques.
- IT resource investment and allocation practices, including prioritization criteria.
- IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships.
- Enterprise risk management.
- Monitoring and reporting of IT performance.
- IT human resources (personnel) management practices used to invoke the business continuity plan.
- Business impact analysis (BIA) related to business continuity planning.
- The standards and procedures for the development and maintenance of the business continuity plan and testing methods.

Domain 3: Information Systems Acquisition, Development, and Implementation
- Benefits realisation practices.
- Project governance mechanisms.
- Project management control frameworks, practices and tools.
- Risk management practices applied to projects.
- IT architecture related to data, applications and technology.
- Acquisition practices.
- Analysis and management practices.
- Analysis and management practices.
- Project success criteria and risks.
- Control objectives and techniques that ensure the completeness, accuracy, validity and authorisation of transactions and data.
- System development methodologies and tools including their strengths and weaknesses.
- Testing methodologies and practices related to information systems development.
- Configuration and release management relating to the development of information systems.
- System migration and infrastructure deployment practices and data conversion tools, techniques and procedures.
- Post-implementation review objectives and practices.

Domain 4: Information Systems Operations, Maintenance and Support
- Service level management practices and the components within a service level agreement.
- Techniques for monitoring third party compliance with the organisation’s internal controls.
- Operations and end-user procedures for managing scheduled and non-scheduled processes.
- Technology concepts related to hardware and network components, system software and database management systems.
- Control techniques that ensure the integrity of system interfaces.
- Software licensing and inventory practices.
- System resiliency tools and techniques.
- Database administration practices.
- Capacity planning and related monitoring tools and techniques.
- Systems performance monitoring processes, tools and techniques.

- Problem and incident management practices.
- Processes, for managing scheduled and non-scheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices.
- Data backup, storage, maintenance, retention and restoration practices.
- Regulatory, legal, contractual and insurance issues related to disaster recovery.
- Business impact analysis (BIA) related to disaster recovery planning.
- Development and maintenance of disaster recovery plans.
- Alternate processing sites and methods used to monitor the contractual agreements.
- Processes used to invoke the disaster recovery plans.
- Disaster recovery testing methods.

Domain 5: Protection of Information Assets

- Techniques for the design, implementation, and monitoring of security controls, including security awareness programs.
- Processes related to monitoring and responding to security incidents.
- Logical access controls for the identification, authentication and restriction of users to authorised functions and data.
- Security controls related to hardware, system software, and database management systems.
- Risks and controls associated with virtualization of systems.
- Configuration, implementation, operation and maintenance of network security controls.
- Network and Internet security devices, protocols, and techniques.
- Information system attack methods and techniques.
- Detection tools and control techniques.
- Security testing techniques.
- Risks and controls associated with data leakage.
- Encryption-related techniques.
- Public key infrastructure (PKI) components and digital signature techniques.
- Risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies.
- Controls and risks associated with the use of mobile & wireless devices.
- Voice communications security.
- Evidence preservation techniques and processes followed in forensics investigations.
- Data classification standards and supporting procedures.
- Physical access controls for the identification, authentication and restriction of users to authorized facilities.
- Environmental protection devices and supporting practices.
- Processes and procedures used to store, retrieve, transport and dispose of confidential information assets.

ENTRY REQUIREMENTS

ISACA requires a minimum of five years' professional information systems auditing, control or security work experience to qualify for full certification. You can take the CISA exam prior to meeting ISACA’s experience requirements, but the CISA qualification will not be awarded until all requirements are met. We do not set specific entry requirements for this course.

THE CISA EXAM

The CISA examination runs a multiple-choice format and consists of a 4-hour paper. The examination tests the candidate’s knowledge of Information System audit principles and practices, as well as technical content areas.

Please note: the exam is not taken during this training course. It needs to be booked directly with

ISACA. There are strict booking dates for the exam, with an advance registration deadline date approximately two months before each course start date.

CISA REVIEW MANUAL

A copy of the current CISA Review Manual is essential for any exam candidate. Unless you already have your own copy, you have the option to purchase the CISA Exam Passport or the CISA Practice Questions Database v14 (Single-User CD-ROM) as part of this course package.