CERTIFIED INFORMATION SYSTEMS AUDITOR

CISA

Duration: 5 days; Instructor-led

OVERVIEW

In this course, you'll cover all five domains of the Certified Information Systems Auditor (CISA) exam and gain the knowledge and technical concepts required to obtain CISA certification. Since its inception in 1978, the CISA exam has become the gold standard of excellence in IS auditing, control, and security. Our experts have created a study guide of relevant, up-to-date information, including summary charts, insightful data, and practice exams.

OBJECTIVES

- Prepare for and pass the Certified Information Systems Auditor (CISA) Exam
- Develop and implement a risk-based IT audit strategy in compliance with IT audit standards
- Evaluate the effectiveness of an IT governance structure
- Ensure that the IT organizational structure and human resources (personnel) management support the organization's strategies and objectives
- Review the information security policies, standards, and procedures for completeness and alignment with generally accepted practices

PREREQUISITES

There are no prerequisite requirements for taking the CISA Exam Preparation Course or the CISA exam; however, in order to apply for CISA certification, the candidate must meet the necessary experience requirements determined by ISACA.

AUDIENCE

- The CISA designation is for Information Systems Audit professionals who have 5 years of front-line experience with the audit of information systems.
- Example are IS / IT auditors, IT managers, Audit Managers, Security Managers, System Analysts, Consultants, and to some extent CIOs and CTOs.

COURSE CONTENTS

Module 1: The Process of Auditing Information Systems

- Develop and implement a risk-based IT audit strategy
- Plan specific audits
- Conduct audits in accordance with IT audit standards
- Report audit findings and make recommendations to key stakeholders
- Conduct follow-ups or prepare status reports

Module 2: IT Governance and Management of IT

- Evaluate the effectiveness of the IT governance structure
- Evaluate IT organizational structure and human resources (personnel) management
- Evaluate the organization's IT policies, standards, and procedures
- Evaluate the adequacy of the quality management system
- Evaluate IT management and monitoring of controls
- Evaluate IT contracting strategies and policies, and contract management practices
- Evaluate risk management practices
- Evaluate the organization's business continuity plan

Module 3: Information Systems Acquisition, Development, and Implementation

- Evaluate the business case for proposed investments in information
- Evaluate the project management practices and controls
- Conduct reviews to determine whether a project is progressing in accordance with project plans
- Evaluate controls for information systems
- Evaluate the readiness of information systems for implementation and migration into production
- Conduct post implementation reviews of systems

Module 4: Information Systems Operations, Maintenance, and Support

- Conduct periodic reviews of information systems
- Evaluate service level management practices
- Evaluate third-party management practices
- Evaluate data administration practices
- Evaluate the use of capacity and performance monitoring tools and techniques
- Evaluate change, configuration, and release management practices

Module 5: Protection of Information Assets

- Evaluate the information security policies, standards and procedures
- Evaluate the design, implementation, and monitoring of system and logical security
- Evaluate the design, implementation, and monitoring of physical access and environmental control
- Evaluate the processes and procedures used to store, retrieve, transport, and dispose of information assets