Certified Information Systems Auditor (CISA)

Duration: 5 Days

Method: Instructor-Led (ILT)

Certification: *Certified Information Systems Auditor (CISA)*

Course Description

This exam preparation course is designed to prepare professionals for the Certified Information Systems Auditor™ (CISA) exam. The course focuses on the key points covered in the CISA Review Manual 26th Edition and includes class lectures, group discussions, exam practice and answer debriefs. The course is intended for individuals with familiarity with and experience in information systems auditing, control or security.

The CISA designation is a globally recognized certification for IS audit control, assurance and security professionals. Being CISA certified showcases your audit experience, skills and knowledge, and demonstrates you are capable to assess vulnerabilities, report on compliance and institute controls within the enterprise.

Target Audience

This course is intended for individuals who audit, control, monitor and assess information technology and business system such as:

- Information systems security professionals, internal review auditors, and other individuals who have an interest in aspects of information systems audit, controls, and security.

Prerequisites

To attend this course, there are no prerequisite requirements for taking the CISA course or the exam; however, in-order-to apply for the CISA certification, the candidate must meet the following requirements as determined by ISACA:

- Five (5) or more years of experience in IS audit, control, assurance, or security
- Waivers are available for a maximum of three (3) years

Exam Details

Exam Tile:	• Certified Information Systems Auditor
Exam Code:	• CISA
Length of Exam:	• 4 Hours
Number of Questions:	• 150
Passing Grade:	• 450 out of 800 points
Availability:	• PSI Testing Center
Question Format:	• Multiple choice and advanced innovative questions

Course Objectives

Upon successful completion of this course, participants will be able to:

- Understand the format and structure of the CISA certification exam
- Have knowledge of the various topics and technical areas covered by the exam
- Practice with specific strategies, tips and techniques for taking and passing the exam

Course Content

Domain 1: The Process of Auditing Information Systems

- Execute a risk-based IS audit strategy in compliance with IS audit standards to ensure that key risk areas are audited
- Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization
- Conduct audits in accordance with IS audit standards to achieve planned audit objectives
- Communicate audit results and make recommendations to key stakeholders through meetings and audit reports to promote change when necessary
- Conduct audit follow-ups to determine whether appropriate actions have been taken by management in a timely manner

Course Content, *Continued*

Domain 2: Governance and Management of IT

- Evaluate the IT strategy, including IT direction, and the processes for the strategy's development, approval, implementation and maintenance, for alignment with the organization's strategies and objectives
- Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives
- Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives
- Evaluate the organization's IT policies, standards and procedures, and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements
- Evaluate IT resource management, including investment, prioritization, allocation and use, for alignment with the organization's strategies and objectives
- Evaluate IT portfolio management, including investment, prioritization and allocation, for alignment with the organization's strategies and objectives
- Evaluate risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed
- Evaluate IT management and monitoring of controls (e.g., continuous monitoring, Quality Assurance [QA]) for compliance with the organization's policies, standards and procedures
- Evaluate monitoring and reporting of IT key performance indicators (KPIs) to determine whether management receives sufficient and timely information
- Evaluate the organization's business continuity plan (BCP), including alignment of the IT disaster recovery plan (DRP) with the BCP, to determine the organization's ability to continue essential business operations during the period of an IT disruption

Domain 3: Information Systems Acquisition, Development and Implementation

- Evaluate the business case for the proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether the business case meets business objectives
- Evaluate IT supplier selection and contract management processes to ensure that the organization's service levels and requisite controls are met
- Evaluate the project management framework and controls to determine whether business requirements are achieved in a cost-effective manner while managing risk to the organization
- Conduct reviews to determine whether a project is progressing in accordance with project plans is adequately supported by documentation and has timely and accurate status reporting
- Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements
- Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and the organization's requirements are met
- Conduct post-implementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met

Course Content, *Continued*

Domain 4: Information Systems Operations, Maintenance and Service Management

- Evaluate the IT service management framework and practices (internal or third party) to determine whether the controls and service levels expected by the organization are being adhered to and whether strategic objectives are met
- Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives within the Enterprise Architecture (EA)
- Evaluate IT operations (e.g., job scheduling, configuration management, capacity and performance management) to determine whether they are controlled effectively and continue to support the organization's objectives
- Evaluate IT maintenance (patches, upgrades) to determine whether they are controlled effectively and continue to support the organization's objectives
- Evaluate database management practices to determine the integrity and optimization of databases.
- Evaluate data quality and lifecycle management to determine whether they continue to meet strategic objectives.
- Evaluate problem and incident management practices to determine whether problems and incidents are prevented, detected, analysed, reported and resolved in a timely manner to support the organization´s objectives
- Evaluate change and release management practices to determine whether changes made to systems and applications are adequately controlled and documented
- Evaluate end-user computing to determine whether the processes are effectively controlled and support the organization's objectives
- Evaluate IT continuity and resilience (backups/restores, Disaster Recovery Plan [DRP]) to determine whether they are controlled effectively and continue to support the organization's objectives

Domain 5: Protection of Information Assets

- Evaluate the information security and privacy policies, standards and procedures for completeness, alignment with generally accepted practices and compliance with applicable external requirements
- Evaluate the design, implementation, maintenance, monitoring and reporting of physical and environmental controls to determine whether information assets are adequately safeguarded
- Evaluate the design, implementation, maintenance, monitoring and reporting of system and logical security controls to verify the confidentiality, integrity and availability of information
- Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements
- Evaluate the processes and procedures used to store, retrieve, transport and dispose of assets to determine whether information assets are adequately safeguarded
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives

LABS INCLUDED