Certified Information Systems Auditor (CISA), 4 Days

Course Summary

Description

An ISACA Certified Information Systems Auditor is recognized as one of the leading authorities in the areas of IS auditing, control, and information security. This official CISA training course provides you with in-depth coverage of the five CISA domains that are covered on the CISA exam. These domains include auditing information systems; IT governance and management of IT; information systems acquisition, development, and implementation; information systems operations, maintenance, and support; and protection of information assets

Objectives

At the completion of this course, Students will:

- 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
- Prepare for and pass the Certified Information Systems Auditor (CISA) Exam, if needed

Topics

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

Prerequisites

IT professionals must have 5 years or more of IS audit, control, assurance and security experience.

Duration

Four Days

Certified Information Systems Auditor (CISA), 4 Days

Course Outline

I. *The Process of Auditing Information Systems*

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

II. *IT Governance and Management of IT*

A. Evaluate the effectiveness of the IT governance structure
B. Evaluate IT organizational structure and human resources (personnel) management
C. Evaluate the organization’s IT policies, standards, and procedures
D. Evaluate the adequacy of the quality management system
E. Evaluate IT management and monitoring of controls
F. Evaluate IT contracting strategies and policies, and contract management practices
G. Evaluate risk management practices
H. Evaluate the organization’s business continuity plan

III. *Information Systems Acquisition, Development, and Implementation*

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

IV. *Information Systems Operations, Maintenance, and Support*

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

V. *Protection of Information Assets*

A. Evaluate the information security policies, standards and procedures
B. Evaluate the design, implementation, and monitoring of system and logical security
C. Evaluate the design, implementation, and monitoring of physical access and environmental controls
D. Evaluate the processes and procedures used to store, retrieve, transport, and dispose of information assets