Certified Information Systems Auditor (CISA)

Duration: 5 days

Course Overview

In this course, students will evaluate organizational policies, procedures, and processes to ensure that an organizations information systems align with its overall business goals and objectives.

Who Should Attend

The intended audience for this course is information systems security professionals, internal review auditors, and other individuals who have an interest in aspects of information systems audit, controls, and security.

Course Objectives

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

 implement information systems audit services in accordance with information systems audit standards, guidelines, and best practices.
 evaluate an organizations structure, policies, accountability, mechanisms, and monitoring practices.
 evaluate information systems acquisition, development, and implementation.
 evaluate the information systems operations, maintenance, and support of an organization; and evaluate the business continuity and disaster recovery processes used to provide assurance that in the event of a disruption, IT services are maintained.
 define the protection policies used to promote the confidentiality, integrity, and availability of information assets.
Course Outline

1 - The Process of Auditing Information Systems

- ISACA Information Systems Auditing Standards and Guidelines
- Fundamental Business Processes
- Develop and Implement an Information Systems Audit Strategy
- Plan an Audit
- Conduct an Audit
- The Evidence Life Cycle
- Communicate Issues, Risks, and Audit Results
- Support the Implementation of Risk Management and Control Practices

2 - IT Governance and Management

- Evaluate the Effectiveness of IT Governance
- Evaluate the IT Organizational Structure and HR Management
- Evaluate the IT Strategy and Direction

- Evaluate IT Policies, Standards, and Procedures
- Evaluate the Effectiveness of Quality Management Systems
- Evaluate IT Management and Monitoring of Controls
- IT Resource Investment, Use, and Allocation Practices
- Evaluate IT Contracting Strategies and Policies
- Evaluate Risk Management Practices
- Performance Monitoring and Assurance Practices
- Evaluate the Organizations Business Continuity Plan

3 - Information Systems Acquisition, Development, and Implementation

- Evaluate the Business Case for Change
- Evaluate Project Management Frameworks and Governance Practices
- Development Life Cycle Management
- Perform Periodic Project Reviews
- Evaluate Control Mechanisms for Systems
- Evaluate Development and Testing Processes
- Evaluate Implementation Readiness
- Evaluate a System Migration
- Perform a Post-Implementation System Review

4 - Information Systems Operations, Maintenance, and Support

- Perform Periodic System Reviews
- Evaluate Service Level Management Practices
- Evaluate Third-Party Management Practices
- Evaluate Operations and End User Management Practices
- Evaluate the Maintenance Process
- Evaluate Data Administration Practices
- Evaluate the Use of Capacity and Performance Monitoring Methods
- Evaluate Change, Configuration, and Release Management Practices
- Evaluate Problem and Incident Management Practices
- Evaluate the Adequacy of Backup and Restore Provisions

5 - Protection of Information Assets

- Information Security Design
- Encryption Basics
- Evaluate the Functionality of the IT Infrastructure
- Evaluate Network Infrastructure Security
- Evaluate the Design, Implementation, and Monitoring of Logical Access Controls
- Risks and Controls of Virtualization
- Evaluate the Design, Implementation, and Monitoring of Data Classification Process
- Evaluate the Design, Implementation, and Monitoring of Physical Access Controls
- Evaluate the Design, Implementation, and Monitoring of Environmental Controls