Course Outline

CISA -Certified Information Systems Auditor

Duration

35 hours

Learning Objectives:

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

Prerequisites

Systems administration experience, familiarity with TCP/IP, and an understanding of UNIX, Linux, and Windows. This advanced course also requires intermediate-level knowledge of the security concepts covered in our Security+ Prep Course.

Target Audience:

IS audit, control, assurance, and security professionals, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers, who have five years of experience with audit, IT systems, and security of information systems.

Topics Covered:

- The Information Systems Audit Process

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

- IT Governance

  - Evaluate the Effectiveness of IT Governance
  - Evaluate the IT Organizational Structure
  - Evaluate the IT Strategy
  - Evaluate IT Policies, Standards, and Procedures for Compliance
  - Ensure Organizational Compliance
  - IT Resource Investment, Use, and Allocation Practices

- Evaluate IT Contracting Strategies and Policies
- Evaluate Risk Management Practices
- Performance Monitoring and Assurance Practices

➢ Systems and Infrastructure Lifecycle Management

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

➢ Systems and Infrastructure Lifecycle Maintenance

- Perform a Post-Implementation System Review
- Perform Periodic System Reviews
- Evaluate the Maintenance Process
- Evaluate the Disposal Process

➢ IT Service Delivery and Support

- Evaluate Service Level Management Practices
- Evaluate Operations Management
- 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 Functionality of the IT Infrastructure

➢ Protection of Information Assets

- Information Security Design
- Encryption Basics
- Evaluate the Design, Implementation, and Monitoring of Logical Access Controls
- Evaluate the Design, Implementation, and Monitoring of Physical Access Controls
- Evaluate the Design, Implementation, and Monitoring of Environmental Controls
- Evaluate Network Infrastructure Security
- Evaluate the Confidential Information Processes and Procedures

➢ Business Continuity and Disaster Recovery

- Evaluate the Adequacy of Backup and Restore
- Evaluate the BCP and DRP

➢ Appendix A: ISACA CISA Certification Process