

Course Outline: Certified Information Systems Auditor (CISA)

Duration: 5 days/30 hours

Who should attend:

- Audit, control, assurance, and security professionals
- IT consultants
- Auditors,
- Managers
- Security policy writers,
- Privacy officers
- Information security officers
- Network administrators
- Security device administrators
- Security engineers

Overview

In this course, you'll cover all six 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.

Objectives:

In-depth coverage of the six domains required to pass the CISA exam:

- IS Audit Process
- IT Governance
- Systems and Infrastructure Lifecycle Management
- IT Service Delivery and Support
- Protection of Information Assets
- Business Continuity and Disaster Recovery

Outline:

Module1: Testing-Taking Tips and Study Techniques

- Preparation for the CISA Exam
- Submitting Required Paperwork
- Resources and Study Aids
- Passing the Exam the First Time

Module 2: The Audit Process

- Risk
- Audit
- Standards and Guidelines

Module 3: IT Governance

- Best Practices
- Management Practices
- Roles and Responsibilities

Module 4: Lifecycle Management

- Project Management
- Business Application Development
- Information Systems Maintenance Practices

- Taxonomy - Information Classification
- Risk Management
- Policies, Procedures, Standards, Guidelines, Baselines
- Knowledge Transfer - Awareness, Training, Education

Module 5: System Infrastructure Control

- Auditing Application Controls
- Application System Development
- Business Application Systems

Module 9: Physical Security

- Environmental Protection Practices
- Physical Authentication
- Policies and Procedures

Module 6: Information Systems Hardware and Architecture

- Information Systems Operations
- Information Systems Hardware
- SDLC
- Databases

Module 10: Business Continuity and Disaster Recovery

- BIA Policy
- BIA Roles and Teams
- Data Backups, Vaulting, Journaling, Shadowing
- Alternate Sites
- Emergency Response
- Required Notifications
- BIA Tests

Module 7: Information Systems Used for IT Delivery and Support

- OSI
- TCP/IP Model
- TCP/UDP/ICMP/IP
- Routers/Switches/Hubs
- Firewalls
- Wireless
- WAN Technologies - X.25/Frame Relay/PPP/ISDN/DSL/Cable

Module 11: Review and Q&A Session

Module 8: Protection of Logical Assets

- CIA
- Roles and Responsibilities - RACI
- Asset Management