ADEPT LEARN

Certified Information Systems Auditor - CISA
Course Duration: 40 Hours (5 Days)

The Certified Information Systems Auditor (CISA) course is a globally recognized certification for IS audit control, assurance, and security professionals. It teaches learners how to assess an organization's information systems and technology and provides the necessary skills to manage and protect information assets effectively. The course is structured into five main domains, each with a series of lessons focusing on different aspects of IS auditing and management. Information Systems Auditing Process covers the essentials of planning and conducting a risk based IS audit strategy, understanding audit standards, and utilizing various audit techniques. Governance and Management of IT ensures learners grasp the importance of IT governance, frameworks, and quality management. The Information Systems Acquisition, Development, and Implementation section addresses how to manage and audit system lifecycles. Information Systems Operations and Business Resilience is about maintaining operations and ensuring business continuity. Lastly, Protection of Information Assets emphasizes the importance of securing data and information systems. Learners who complete the CISA course will be equipped with critical skills for IT governance, system auditing, and security management, significantly enhancing their professional credibility and career opportunities in the field of information systems audit.

Audience profile

The CISA course equips IT professionals with skills to manage and protect information systems in organizations.

- IT Auditors
- Information Security Analysts
- Information Systems Control Professionals
- Chief Information Officers (CIOs)
- Chief Technology Officers (CTOs)
- IT Risk Managers
- Security Consultants
- Compliance Officers
- IT Assurance Professionals
- Cybersecurity Professionals
- Corporate IT Governance Managers
- Quality Assurance (QA) Managers
- IT Consultants
- Network Operation Security Engineers
- IS/IT Consultants
- IT Project Managers
- Regulatory Compliance Managers
- Data Privacy Officers
- IT Forensic Investigators
- Systems Analysts or Developers with a focus on security and compliance

Course Syllabus
Domain 1: Information Systems Auditing Process - (21%)

Planning
- IS Audit Standards, Guidelines, and Codes of Ethics
- Business Processes
- Types of Controls
- Risk-Based Audit Planning
- Types of Audits and Assessments

Execution
- Audit Project Management
- Sampling Methodology
- Audit Evidence Collection Techniques
- Data Analytics
- Reporting and Communication Techniques

Domain 2: Governance and Management of IT - (17%)
Domain 2 confirms to stakeholders your abilities to identify critical issues and recommend enterprise-specific practices to support and safeguard the governance of information and related technologies.

IT Governance
- IT Governance and IT Strategy
- IT-Related Frameworks
- IT Standards, Policies, and Procedures
- Organizational Structure
- Enterprise Architecture
- Enterprise Risk Management
- Maturity Models
- Laws, Regulations, and Industry Standards affecting the Organization

IT Management
- IT Resource Management
- IT Service Provider Acquisition and Management
- IT Performance Monitoring and Reporting
- Quality Assurance and Quality Management of IT

Domain 3: Information Systems Acquisition, Development and Implementation - (12%)

Information Systems Acquisition and Development
- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies
- Control Identification and Design

Information Systems Implementation
- Testing Methodologies
- Configuration and Release Management
- System Migration, Infrastructure Deployment, and Data Conversion
- Post-implementation Review

Domain 4: Information Systems Operations and Business Resilience - (23%)
Domains 3 and 4 offer proof not only of your competency in IT controls, but also your understanding of how IT relates to business.

Information Systems Operations
- Common Technology Components
- IT Asset Management
- Job Scheduling and Production Process Automation
- System Interfaces
- End-User Computing
- Data Governance
- Systems Performance Management
- Problem and Incident Management
- Change, Configuration, Release, and Patch Management
- IT Service Level Management
- Database Management

Business Resilience
- Business Impact Analysis (BIA)
- System Resiliency
- Data Backup, Storage, and Restoration
- Business Continuity Plan (BCP)
- Disaster Recovery Plans (DRP)

Domain 5: Protection of Information Assets - (27%)
Cybersecurity now touches virtually every information systems role, and understanding its principles, best practices and pitfalls is a major focus within Domain 5.

Information Asset Security and Control
- Information Asset Security Frameworks, Standards, and Guidelines
- Privacy Principles
- Physical Access and Environmental Controls
- Identity and Access Management
- Network and End-Point Security
- Data Classification
- Data Encryption and Encryption-Related Techniques
- Public Key Infrastructure (PKI)
- Web-Based Communication Techniques
- Virtualized Environments
- Mobile, Wireless, and Internet-of-Things (IoT) Devices

Security Event Management
- Security Awareness Training and Programs
- Information System Attack Methods and Techniques
- Security Testing Tools and Techniques
- Security Monitoring Tools and Techniques
- Incident Response Management
- Evidence Collection and Forensics