Certified Information Systems Auditor-CISA

Duration: 5 Days

Prerequisites:

To ensure that you have a successful learning experience in the Certified Information Systems Auditor (CISA) course, the following minimum prerequisites are recommended:

- Understanding of Basic IT Concepts: Familiarity with general IT terminology and concepts to comprehend technical discussions within the course.
- Awareness of Business Processes: Basic knowledge of how businesses operate, including an understanding of common business processes and the role of information systems in supporting them.
- Experience in IT or Audit: Although not mandatory, having some prior experience in IT, cybersecurity, or audit-related roles can be highly beneficial for grasping the course content more effectively.
- Analytical Skills: Ability to analyze and interpret information, as auditing involves assessing complex systems and processes to identify risks and control weaknesses.
- Ethical Mindset: A strong sense of ethics and integrity, as the course covers codes of ethics that are crucial for auditors.
- Commitment to Professional Development: A willingness to engage in continuous learning and professional development, as the field of information systems auditing is constantly evolving.
- Proficiency in English: Ability to read, write, and comprehend English, as the course materials and the CISA certification exam are presented in English.
- Remember, these are the minimum requirements to help ensure you can effectively participate in the CISA course. Your dedication and willingness to learn will also play a significant role in the successful completion of the training.

Course Objectives:

- Develop a solid grasp of planning and executing information systems audits in accordance with IS audit standards, guidelines, and codes of ethics.
- Understand how to evaluate the effectiveness of IT governance, including strategy alignment, resource management, and performance monitoring.
- Acquire skills to assess risks and controls within business processes and information systems and propose enhancements.
- Learn to manage IT-related frameworks and ensure compliance with laws, regulations, and industry standards.
- Gain proficiency in overseeing information systems acquisition, development, and implementation projects, including project management and system migration.
- Master the concepts of information systems operations, including common technology components, IT asset management, and systems performance management.
- Enhance business resilience by learning how to conduct business impact analysis and develop effective business continuity and disaster recovery plans.
- Attain expertise in protecting information assets through security frameworks, identity and access management, and encryption techniques.
- Learn to identify and respond to security events using appropriate security testing and monitoring tools, and incident response management.
- Prepare to collect and handle audit evidence and understand the principles of forensic investigation to support legal and organizational objectives.

Course Description:

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.

Target Audience:

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 Outline:

Module 1: INFORMATION SYSTEMS AUDITING PROCESS - (21%)

Providing audit services in accordance with standards to assist organizations in protecting and controlling information systems. Domain 1 affirms your credibility to offer conclusions on the state of an organization's IS/IT security, risk and control solutions.

- Planning
- Execution

Module 2: Governance and Management of IT - (17%)

Module 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 Management

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

- Information Systems Acquisition and Development
- Information Systems Implementation

Module 4: INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE- (23%)

Module 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
- Business Resilience

Module 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 Module 5.

- Information Asset Security and Control
- Security Event Management