Certified Information Systems Auditor Preparation

Course Description

Build your information security career up to the top by achieving CISA qualification. This course will provide you with required knowledge to be an information security/cyber security professional in audit, assurance, control and consultancy.

CISA qualification is the globally recognized security certification, being CISA certified represent your audit experience, skills and knowledge and capabilities in overall information security, vulnerabilities assessment, report on compliance and implement controls within the enterprise.

The course will embed you with extend, yet comprehensive for the key job practice domains as well as exam preparation guides and exercises that help candidates who plan to sit in the exam.

Course Objectives

Upon completion of this course, you will be able to understand concept of information security and cyber security which focus on the process of auditing information systems, governance and management of IT, information systems acquisition, development and implementation and information systems operations and business resilience.

The course will help embed you with appropriate skill and knowledge to:

- Audit or consult in information security and cyber security program
- Explain and provide a key critical success factors in governance of IT
- Provide an appropriate practice in information systems development life cycle
- Operate information system to support business resilience

Course Outline

Day 1: Information System Auditing Process

- Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization
- Conduct an audit in accordance with IS audit standards and a risk based IS audit strategy
- Communicate audit progress, findings, results and recommendations to stakeholders
- Conduct audit follow-up to evaluate whether risk has been sufficiently addressed
- Evaluate IT management and monitoring of controls
- Utilize data analytics tools to streamline audit processes
- Provide consulting services and guidance to the organization in order to improve the quality and control of information systems
- Identify opportunities for process improvement in the organization's IT policies and practices

Day 2: Governance & Management of IT

- Evaluate the IT strategy for alignment with the organization's strategies and objectives
- Evaluate the effectiveness of IT governance structure and IT organizational structure
- Evaluate the organization's management of IT policies and practices
- Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements
- Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives
- Evaluate the organization's risk management policies and practices
- Evaluate IT management and monitoring of controls
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs)
- Evaluate whether IT supplier selection and contract management processes align with business requirements
- Evaluate whether IT service management practices align with business requirements
- Conduct periodic review of information systems and enterprise architecture
- Evaluate data governance policies and practices
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices

Day 3: Information Systems Acquisition, Development, & Implementation

- Evaluate whether the business case for proposed changes to information systems meet business objectives
- Evaluate the organization's project management policies and practices
- Evaluate controls at all stages of the information systems development life cycle
- Evaluate the readiness of information systems for implementation and migration into production
- Conduct post-implementation review of systems to determine whether project deliverables, controls and requirements are met
- Evaluate change, configuration, release, and patch management policies and practices

Day 4: Information Systems Operations and Business Resilience

- Evaluate the organization's ability to continue business operations
- Evaluate whether IT service management practices align with business requirements
- Conduct periodic review of information systems and enterprise architecture
- Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives
- Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives
- Evaluate database management practices
- Evaluate data governance policies and practices
- Evaluate problem and incident management policies and practices
- Evaluate change, configuration, release, and patch management policies and practices
- Evaluate end-user computing to determine whether the processes are effectively controlled

Day 5: Protection of Information Assets

- Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy
- Evaluate problem and incident management policies and practices
- Evaluate the organization's information security and privacy policies and practices
- Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded
- Evaluate logical security controls to verify the confidentiality, integrity, and availability of information
- Evaluate data classification practices for alignment with the organization's policies and applicable external requirements
- Evaluate policies and practices related to asset life cycle management
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives
- Perform technical security testing to identify potential threats and vulnerabilities
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices

Who Should Attend?

The primary audiences for this course are as follow:

- Experienced practitioners, managers, and executives those required the skillset of information security, cyber security, information systems auditing and control
- Information security professionals
- Risk management professionals
- Internal and external IT auditors and Compliance officers
- Security Engineer, Professional in IS/IT and related field.
- Individual who interested in advanced certification in information security and cyber security as an opportunity for career enhancement and development.

Course Duration

5 days