learnfly™ | Pro
Up-skill Yourself

Certified Information Systems Auditor (CISA)

Course Details:

Domain 1—The Process of Auditing Information Systems

Provide audit services in accordance with IT audit standards to assist the organization in protecting and controlling information systems.

- ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of
- Professional ethics and other applicable standards.
- Risk assessment concepts, tools and techniques in an audit context.
- Control objectives and controls related to information systems.
- Audit planning and audit project management techniques, including follow-up.
- Fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) including relevant IT.
- Applicable laws and regulations which affect the scope, evidence collection and preservation, and frequency of audits.
- Evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, fraud, investigation) used to gather, protect and preserve audit evidence different sampling methodologies.
- Reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure).
- Audit quality assurance systems and frameworks.

Domain 2—Governance and Management of IT

Provide assurance that the necessary leadership and organization structure and processes are in place to achieve objectives and to support the organization's strategy.

- IT governance, management, security and control frameworks, and related standards, guidelines, and practices
- The purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each organizational structure, roles and responsibilities related to IT.
- The processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
- The organization’s technology direction and IT architecture and their implications for setting long term strategic directions
- Relevant laws, regulations and industry standards affecting the organization
- Quality management systems
- The use of maturity models
- Process optimization techniques

- IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, project management)
- IT supplier selection, contract management, relationship management and performance monitoring
- Processes including third party outsourcing relationships
- Enterprise risk management
- Practices for monitoring and reporting of IT performance (e.g., balanced scorecards, key performance indicators [KPI])
- IT human resources (personnel) management practices used to invoke the business continuity plan
- Business impact analysis (BIA) related to business continuity planning
- The standards and procedures for the development and maintenance of the business continuity plan and testing methods

Domain 3—Information Systems Acquisition, Development, and Implementation

Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization's strategies and objectives.

- Benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], ROI) project governance mechanisms (e.g., steering committee, project oversight board, project management office)
- Project management control frameworks, practices and tools
- Risk management practices applied to projects
- IT architecture related to data, applications and technology (e.g., distributed applications, web based applications, web services, n-tier applications)
- Acquisition practices (e.g., evaluation of vendors, vendor management, escrow)
- Requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements)
- Project success criteria and risks
- Objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data
- System development methodologies and tools including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques)
- Testing methodologies and practices related to information systems development
- Configuration and release management relating to the development of information systems
- System migration and infrastructure deployment practices and data conversion tools, techniques and procedures.
- Post-implementation review objectives and practices (e.g., project closure, control implementation, benefits realization, performance measurement)

Domain 4—Information Systems Operations, Maintenance and Support

Provide assurance that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives.

- Service level management practices and the components within a service level agreement
- Techniques for monitoring third party compliance with the organization's internal controls
- Operations and end-user procedures for managing scheduled and non-scheduled processes
- The technology concepts related to hardware and network components, system software and database management systems
- Control techniques that ensure the integrity of system interfaces
- Software licensing and inventory practices
- System resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)
- Database administration practices
- Capacity planning and related monitoring tools and techniques
- Systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)
- Problem and incident management practices (e.g., help desk, escalation procedures, tracking)
- Processes, for managing scheduled and non-scheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices
- Data backup, storage, maintenance, retention and restoration practices
- Regulatory, legal, contractual and insurance issues related to disaster recovery
- Business impact analysis (BIA) related to disaster recovery planning
- The development and maintenance of disaster recovery plans
- Types of alternate processing sites and methods used to monitor the contractual agreements (e.g., hot sites, warm sites, cold sites)
- Processes used to invoke the disaster recovery plans
- Disaster recovery testing methods

Domain 5—Protection of Information Assets

Provide assurance that the organization's security policies, standards, procedures and controls ensure the confidentiality, integrity and availability of information assets.

- Techniques for the design, implementation, and monitoring of security controls, including security awareness programs
- Processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
- Logical access controls for the identification, authentication and restriction of users to authorized functions and data
- The security controls related to hardware, system software (e.g., applications, operating systems), and database management systems.
- Risks and controls associated with virtualization of systems

- The configuration, implementation, operation and maintenance of network security controls
- Network and Internet security devices, protocols, and techniques
- Information system attack methods and techniques
- Detection tools and control techniques (e.g., malware, virus detection, spyware)
- Security testing techniques (e.g., intrusion testing, social engineering testing, vulnerability scanning)
- Risks and controls associated with data leakage
- Encryption-related techniques
- Public key infrastructure (PKI) components and digital signature techniques
- Risks and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs)
- Controls and risks associated with the use of mobile & wireless devices
- Voice communications security (e.g., PBX, VoIP)
- The evidence preservation techniques and processes followed in forensics investigations (e.g., IT, process, chain of custody, fraud evidence collection)
- Data classification standards and supporting procedures
- Physical access controls for the identification, authentication and restriction of users to authorized facilities environmental protection devices and supporting practices
- The processes and procedures used to store, retrieve, transport and dispose of confidential information assets