Certified Information Systems Auditor (CISA)

Duration: 5 Days

Course Outline

Domain 1 - The Process of Auditing Information Systems

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

Domain 1 - Task Statements:

- 1.1 Execute a risk-based IS audit strategy in compliance with IS audit standards to ensure that key risk areas are audited.
- 1.2 Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization.
- 1.3 Conduct audits in accordance with IS audit standards to achieve planned audit objectives.
- 1.4 Communicate audit results and make recommendations to key stakeholders through meetings and audit reports to promote change when necessary.
- 1.5 Conduct audit follow-ups to determine whether appropriate actions have been taken by management in a timely manner.

Domain 1 - Knowledge Statements:

- 1.1 Knowledge of ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques, Code of Professional Ethics and other applicable standards
- 1.2 Knowledge of the risk assessment concepts and tools and techniques used in planning, examination, reporting and follow-up
- 1.3 Knowledge of fundamental business processes (e.g., purchasing, payroll, accounts payable, accounts receivable) and the role of IS in these processes
- 1.4 Knowledge of the control principles related to controls in information systems
- 1.5 Knowledge of risk-based audit planning and audit project management techniques, including follow-up
- 1.6 Knowledge of the applicable laws and regulations that affect the scope, evidence collection and preservation, and frequency of audits
- 1.7 Knowledge of the evidence collection techniques (e.g., observation, inquiry, inspection, interview, data analysis, forensic investigation techniques, computer-assisted audit techniques [CAATs]) used to gather, protect and preserve audit evidence
- 1.8 Knowledge of different sampling methodologies and other substantive/data analytical procedures
- 1.9 Knowledge of reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification)
- 1.10 Knowledge of audit quality assurance (QA) systems and frameworks
- 1.11 Knowledge of various types of audits (e.g., internal, external, financial) and methods for assessing and placing reliance on the work of other auditors or control entities

Domain 2 - Governance and Management of IT

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

Domain 2 - Task Statements:

- 2.1 Evaluate the IT strategy, including IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
- 2.2 Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.
- 2.3 Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
- 2.4 Evaluate the organization's IT policies, standards and procedures, and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements.
- 2.5 Evaluate IT resource management, including investment, prioritization, allocation and use, for alignment with the organization's strategies and objectives.
- 2.6 Evaluate IT portfolio management, including investment, prioritization and allocation, for alignment with the organization's strategies and objectives.
- 2.7 Evaluate risk management practices to determine whether the organization's IT-related risk is identified, assessed, monitored, reported and managed.
- 2.8 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance [QA]) for compliance with the organization's policies, standards and procedures.
- 2.9 Evaluate monitoring and reporting of IT key performance indicators (KPIs) to determine whether management receives enough and timely information.
- 2.10 Evaluate the organization's business continuity plan (BCP), including alignment of the IT disaster recovery plan (DRP) with the BCP, to determine the organization's ability to continue essential business operations during the period of an IT disruption.

Domain 2 - Knowledge Statements:

- 2.1 Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each
- 2.2 Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines and practices
- 2.3 Knowledge of the organizational structure, roles and responsibilities related to IT, including segregation of duties (SoD)
- 2.4 Knowledge of the relevant laws, regulations and industry standards affecting the organization
- 2.5 Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions
- 2.6 Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
- 2.7 Knowledge of the use of capability and maturity models
- 2.8 Knowledge of process optimization techniques

- 2.9 Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management)
- 2.10 Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes, including third-party outsourcing relationships
- 2.11 Knowledge of enterprise risk management (ERM)
- 2.12 Knowledge of the practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA])
- 2.13 Knowledge of quality management and quality assurance (QA) systems
- 2.14 Knowledge of the practices for monitoring and reporting of IT performance (e.g., balanced scorecard [BSC], key performance indicators [KPIs])
- 2.15 Knowledge of business impact analysis (BIA)
- 2.16 Knowledge of the standards and procedures for the development, maintenance and testing of the business continuity plan (BCP)
- 2.17 Knowledge of the procedures used to invoke and execute the business continuity plan (BCP) and return to normal operations

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.

Domain 3 - Task Statements:

- 3.1 Evaluate the business case for the proposed investments in information systems acquisition, development, maintenance and subsequent retirement to determine whether the business case meets business objectives.
- 3.2 Evaluate IT supplier selection and contract management processes to ensure that the organization's service levels and requisite controls are met.
- 3.3 Evaluate the project management framework and controls to determine whether business requirements are achieved in a cost-effective manner while managing risk to the organization.
- 3.4 Conduct reviews to determine whether a project is progressing in accordance with project plans, is adequately supported by documentation, and has timely and accurate status reporting.
- 3.5 Evaluate controls for information systems during the requirements, acquisition, development and testing phases for compliance with the organization's policies, standards, procedures and applicable external requirements.
- 3.6 Evaluate the readiness of information systems for implementation and migration into production to determine whether project deliverables, controls and the organization's requirements are met.
- 3.7 Conduct post-implementation reviews of systems to determine whether project deliverables, controls and the organization's requirements are met.

Domain 3 - Knowledge Statements:

- 3.1 Knowledge of benefits realization practices, (e.g., feasibility studies, business cases, total cost of ownership [TCO], return on investment [ROI])
- 3.2 Knowledge of IT acquisition and vendor management practices (e.g., evaluation and selection process, contract management, vendor risk and relationship management, escrow,

software licensing), including third-party outsourcing relationships, IT suppliers and service providers.

- 3.3 Knowledge of project governance mechanisms (e.g., steering committee, project oversight board, project management office)
- 3.4 Knowledge of project management control frameworks, practices and tools
- 3.5 Knowledge of the risk management practices applied to projects
- 3.6 Knowledge of requirements analysis and management practices (e.g., requirements verification, traceability, gap analysis, vulnerability management, security requirements)
- 3.7 Knowledge of the enterprise architecture (EA) related to data, applications and technology (e.g., web-based applications, web services, n-tier applications, cloud services, virtualization)
- 3.8 Knowledge of system development methodologies and tools, including their strengths and weaknesses (e.g., agile development practices, prototyping, rapid application development [RAD], object-oriented design techniques, secure coding practices, system version control)
- 3.9 Knowledge of the control objectives and techniques that ensure the completeness, accuracy, validity and authorization of transactions and data
- 3.10 Knowledge of the testing methodologies and practices related to the information system development life cycle (SDLC)
- 3.11 Knowledge of the configuration and release management relating to the development of information systems
- 3.12 Knowledge of system migration and infrastructure deployment practices and data conversion tools, techniques and procedures.
- 3.13 Knowledge of project success criteria and project risk
- 3.14 Knowledge of post-implementation review objectives and practices (e.g., project closure, control implementation, benefits realization, performance measurement)

Domain 4 - Information Systems Operations, Maintenance and Service Management

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

Domain 4 - Task Statements:

- 4.1 Evaluate the IT service management framework and practices (internal or third party) to determine whether the controls and service levels expected by the organization are being adhered to and whether strategic objectives are met.
- 4.2 Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives within the enterprise architecture (EA).
- 4.3 Evaluate IT operations (e.g., job scheduling, configuration management, capacity and performance management) to determine whether they are controlled effectively and continue to support the organization's objectives.
- 4.4 Evaluate IT maintenance (patches, upgrades) to determine whether they are controlled effectively and continue to support the organization's objectives.
- 4.5 Evaluate database management practices to determine the integrity and optimization of databases.
- 4.6 Evaluate data quality and life cycle management to determine whether they continue to meet strategic objectives.

- 4.7 Evaluate problem and incident management practices to determine whether problems and incidents are prevented, detected, analyzed, reported and resolved in a timely manner to support the organization's objectives.
- 4.8 Evaluate change and release management practices to determine whether changes made to systems and applications are adequately controlled and documented.
- 4.9 Evaluate end-user computing to determine whether the processes are effectively controlled and support the organization's objectives.
- 4.10 Evaluate IT continuity and resilience (backups/restores, disaster recovery plan [DRP]) to determine whether they are controlled effectively and continue to support the organization's objectives.

Domain 4 - Knowledge Statements:

- 4.1 Knowledge of service management frameworks
- 4.2 Knowledge of service management practices and service level management
- 4.3 Knowledge of the techniques for monitoring third-party performance and compliance with service agreements and regulatory requirements
- 4.4 Knowledge of enterprise architecture (EA)
- 4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)
- 4.6 Knowledge of system resiliency tools and techniques (e.g., fault-tolerant hardware, elimination of single point of failure, clustering)
- 4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices
- 4.8 Knowledge of job scheduling practices, including exception handling
- 4.9 Knowledge of the control techniques that ensure the integrity of system interfaces
- 4.10 Knowledge of capacity planning and related monitoring tools and techniques
- 4.11 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)
- 4.12 Knowledge of data backup, storage, maintenance and restoration practices
- 4.13 Knowledge of database management and optimization practices
- 4.14 Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)
- 4.15 Knowledge of problem and incident management practices
- 4.16 Knowledge of change management, configuration management, release management and patch management practices
- 4.17 Knowledge of the operational risk and controls related to end-user computing
- 4.18 Knowledge of the regulatory, legal, contractual and insurance issues related to disaster recovery
- 4.19 Knowledge of business impact analysis (BIA) related to disaster recovery planning
- 4.20 Knowledge of the development and maintenance of disaster recovery plans (DRPs)
- 4.21 Knowledge of the benefits and drawbacks of alternate processing sites (e.g., hot sites, warm sites, cold sites)
- 4.22 Knowledge of disaster recovery testing methods
- 4.23 Knowledge of the processes used to invoke the disaster recovery plans (DRPs)

Domain 5—Protection of Information Assets

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

Domain 5 - Task Statements:

- 5.1 Evaluate the information security and privacy policies, standards and procedures for completeness, alignment with generally accepted practices and compliance with applicable external requirements.
- 5.2 Evaluate the design, implementation, maintenance, monitoring and reporting of physical and environmental controls to determine whether information assets are adequately safeguarded.
- 5.3 Evaluate the design, implementation, maintenance, monitoring and reporting of system and logical security controls to verify the confidentiality, integrity and availability of information.
- 5.4 Evaluate the design, implementation and monitoring of the data classification processes and procedures for alignment with the organization's policies, standards, procedures and applicable external requirements.
- 5.5 Evaluate the processes and procedures used to store, retrieve, transport and dispose of assets to determine whether information assets are adequately safeguarded.
- 5.6 Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.

Domain 5 - Knowledge Statements:

- 5.1 Knowledge of the generally accepted practices and applicable external requirements (e.g., laws, regulations) related to the protection of information assets
- 5.2 Knowledge of privacy principles
- 5.3 Knowledge of the techniques for the design, implementation, maintenance, monitoring and reporting of security controls
- 5.4 Knowledge of the physical and environmental controls and supporting practices related to the protection of information assets
- 5.5 Knowledge of the physical access controls for the identification, authentication and restriction of users to authorized facilities and hardware
- 5.6 Knowledge of the logical access controls for the identification, authentication and restriction of users to authorized functions and data
- 5.7 Knowledge of the security controls related to hardware, system software (e.g., applications, operating systems) and database management systems.
- 5.8 Knowledge of the risk and controls associated with virtualization of systems
- 5.9 Knowledge of the risk and controls associated with the use of mobile and wireless devices, including personally owned devices (bring your own device [BYOD])
- 5.10 Knowledge of voice communications security (e.g., PBX, Voice-over Internet Protocol [VoIP])
- 5.11 Knowledge of network and Internet security devices, protocols and techniques
- 5.12 Knowledge of the configuration, implementation, operation and maintenance of network security controls
- 5.13 Knowledge of encryption-related techniques and their uses
- 5.14 Knowledge of public key infrastructure (PKI) components and digital signature techniques

- 5.15 Knowledge of the risk and controls associated with peer-to-peer computing, instant messaging, and web-based technologies (e.g., social networking, message boards, blogs, cloud computing)
- 5.16 Knowledge of the data classification standards related to the protection of information assets
- 5.17 Knowledge of the processes and procedures used to store, retrieve, transport and dispose of confidential information assets
- 5.18 Knowledge of the risk and controls associated with data leakage
- 5.19 Knowledge of the security risk and controls related to end-user computing
- 5.20 Knowledge of methods for implementing a security awareness program
- 5.21 Knowledge of information system attack methods and techniques
- 5.22 Knowledge of prevention and detection tools and control techniques
- 5.23 Knowledge of security testing techniques (e.g., penetration testing, vulnerability scanning)
- 5.24 Knowledge of the processes related to monitoring and responding to security incidents (e.g., escalation procedures, emergency incident response team)
- 5.25 Knowledge of the processes followed in forensics investigation and procedures in collection and preservation of the data and evidence (i.e., chain of custody).
- 5.26 Knowledge of the fraud risk factors related to the protection of information assets