CISA - Certified Information Systems Auditor

Course Outline

Domain 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.

A. Planning

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

B. 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.

A. 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

B. 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%)

A. Information Systems Acquisition and Development

- Project Governance and Management
- Business Case and Feasibility Analysis
- System Development Methodologies

- Control Identification and Design

B. 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.

A. 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

B. 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.

A. 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

B. 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

Supporting Tasks

1. Plan audit to determine whether information systems are protected, controlled, and provide value to the organization.
2. Conduct audit in accordance with IS audit standards and a risk-based IS audit strategy.
3. Communicate audit progress, findings, results, and recommendations to stakeholders.
4. Conduct audit follow-up to evaluate whether risks have been sufficiently addressed.
5. Evaluate the IT strategy for alignment with the organization's strategies and objectives.
6. Evaluate the effectiveness of IT governance structure and IT organizational structure.
7. Evaluate the organization's management of IT policies and practices.
8. Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements.
9. Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives.
10. Evaluate the organization's risk management policies and practices.
11. Evaluate IT management and monitoring of controls.
12. Evaluate the monitoring and reporting of IT key performance indicators (KPIs).
13. Evaluate the organization's ability to continue business operations.
14. Evaluate whether the business case for proposed changes to information systems meets business objectives.
15. Evaluate whether IT supplier selection and contract management processes align with business requirements.
16. Evaluate the organization's project management policies and practices.
17. Evaluate controls at all stages of the information systems development lifecycle.
18. Evaluate the readiness of information systems for implementation and migration into production.
19. Conduct post-implementation review of systems to determine whether project deliverables, controls, and requirements are met.
20. Evaluate whether IT service management practices align with business requirements.
21. Conduct periodic review of information systems and enterprise architecture.
22. Evaluate IT operations to determine whether they are controlled effectively and continue to support the organization's objectives.
23. Evaluate IT maintenance practices to determine whether they are controlled effectively and continue to support the organization's objectives.
24. Evaluate database management practices.
25. Evaluate data governance policies and practices.

---

26. Evaluate problem and incident management policies and practices.
27. Evaluate change, configuration, release, and patch management policies and practices.
28. Evaluate end-user computing to determine whether the processes are effectively controlled.
29. Evaluate the organization's information security and privacy policies and practices.
30. Evaluate physical and environmental controls to determine whether information assets are adequately safeguarded.
31. Evaluate logical security controls to verify the confidentiality, integrity, and availability of information.
32. Evaluate data classification practices for alignment with the organization's policies and applicable external requirements.
33. Evaluate policies and practices related to asset lifecycle management.
34. Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives.
35. Perform technical security testing to identify potential threats and vulnerabilities.
36. Utilize data analytics tools to streamline audit processes.
37. Provide consulting services and guidance to the organization in order to improve the quality and control of information systems.
38. Identify opportunities for process improvement in the organization's IT policies and practices.
39. Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices.