Appendix A

CISA Examination Content Outline

(Effective August 2024)

1	**Information System Auditing Process**
A	Planning
1	IS Audit Standards, Guidelines, Functions, and Codes of Ethics
2	Types of Audits, Assessments, and Reviews
3	Risk-Based Audit Planning
4	Types of Controls and Considerations
B	Execution
1	Audit Project Management
2	Audit Testing and Sampling Methodology
3	Audit Evidence Collection Techniques
4	Audit Data Analytics (including audit algorithms)
5	Reporting and Communication Techniques
6	Quality Assurance and Improvement of Audit Process
2	**Governance and Management of IT**
A	IT Governance
1	Laws, Regulations, and Industry Standards
2	Organizational Structure, IT Governance, and IT Strategy
3	IT Policies, Standards, Procedures and Practices
4	Enterprise Architecture (EA) and Considerations
5	Enterprise Risk Management (ERM)
6	Privacy Program and Principles
7	Data Governance and Classification
B	IT Management
1	IT Resource Management
2	IT Vendor Management
3	IT Performance Monitoring and Reporting
4	Quality Assurance and Quality Management of IT
3	**Information Systems Acquisition, Development, and Implementation**
A	Information Systems Acquisition and Development
1	Project Governance and Management
2	Business Case and Feasibility Analysis
3	System Development Methodologies
4	Control Identification and Design
B	Information Systems Implementation
1	System Readiness and Implementation Testing
2	Implementation Configuration and Release Management
3	System Migration, Infrastructure Deployment, and Data Conversion
4	Post-Implementation Review

4	**Information Systems Operations and Business Resilience**
A	Information Systems Operations
1	IT Components
2	IT Asset Management
3	Job Scheduling and Production Process Automation
4	System Interfaces
5	Shadow IT and End-User Computing (EUC)
6	Systems Availability and Capacity Management
7	Problem and Incident Management
8	IT Change, Configuration, and Patch Management
9	Operational Log Management
10	IT Service Level Management
11	Database Management
B	Business Resilience
1	Business Impact Analysis (BIA)
2	System and Operational Resilience
3	Data Backup, Storage, and Restoration
4	Business Continuity Plan (BCP)
5	Disaster Recovery Plans (DRP)
5	**Protection of Information Assets**
A	Information Asset Security and Control
1	Information Asset Security Policies, Frameworks, Standards, and Guidelines
2	Physical and Environmental Controls
3	Identity and Access Management
4	Network and End-Point Security
5	Data Loss Prevention (DLP)
6	Data Encryption
7	Public Key Infrastructure (PKI)
8	Cloud and Virtualized Environments
9	Mobile, Wireless, and Internet-of-Things (IoT) Devices
B	Security Event Management
1	Security Awareness Training and Programs
2	Information System Attack Methods and Techniques
3	Security Testing Tools and Techniques
4	Security Monitoring Logs, Tools, and Techniques
5	Security Incident Response Management
6	Evidence Collection and Forensics

Supporting Tasks

1. Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
2. Conduct audits in accordance with IS audit standards and a risk based IS audit strategy.
3. Apply project management methodologies to the audit process.
4. Communicate and collect feedback on audit progress, findings, results, and recommendations with stakeholders.
5. Conduct post-audit follow up to evaluate whether identified risk has been sufficiently addressed.
6. Utilize data analytics tools to enhance audit processes.
7. Evaluate the role and/or impact of automatization and/or decision-making systems for an organization.
8. Evaluate audit processes as part of quality assurance and improvement programs.
9. Evaluate the IT strategy for alignment with the organization's strategies and objectives.
10. Evaluate the effectiveness of IT governance structure and IT organizational structure.
11. Evaluate the organization's management of IT policies and practices, including compliance with legal and regulatory requirements.
12. Evaluate IT resource and project management for alignment with the organization's strategies and objectives.
13. Evaluate the organization's enterprise risk management (ERM) program.
14. Determine whether the organization has defined ownership of IT risk, controls, and standards.
15. Evaluate the monitoring and reporting of IT key performance indicators (KPIs) and IT key risk indicators (KRIs).
16. Evaluate the organization's ability to continue business operations.
17. Evaluate the organization's storage, backup, and restoration policies and processes.
18. Evaluate whether the business cases related to information systems meet business objectives.
19. Evaluate whether IT vendor selection and contract management processes meet business, legal, and regulatory requirements.
20. Evaluate supply chains for IT risk factors and integrity issues.
21. Evaluate controls at all stages of the information systems development life cycle.
22. Evaluate the readiness of information systems for implementation and migration into production.
23. Conduct post-implementation reviews of systems to determine whether project deliverables, controls, and requirements are met.
24. Evaluate whether effective processes are in place to support end users.
25. Evaluate whether IT service management practices align with organizational requirements.
26. Conduct periodic review of information systems and enterprise architecture (EA) to determine alignment with organizational objectives.
27. Evaluate whether IT operations and maintenance practices support the organization's objectives.
28. Evaluate the organization's database management practices.
29. Evaluate the organization's data governance program.
30. Evaluate the organization's privacy program.
31. Evaluate data classification practices for alignment with the organization's data governance program, privacy program, and applicable external requirements.
32. Evaluate the organization's problem and incident management program.
33. Evaluate the organization's change, configuration, release, and patch management programs.
34. Evaluate the organization's log management program.
35. Evaluate the organization's policies and practices related to asset life cycle management.

36. Evaluate risk associated with shadow IT and end-user computing (EUC) to determine effectiveness of compensating controls.
37. Evaluate the organization's information security program.
38. Evaluate the organization's threat and vulnerability management program.
39. Utilize technical security testing to identify potential vulnerabilities.
40. Evaluate logical, physical, and environmental controls to verify the confidentiality, integrity, and availability of information assets.
41. Evaluate the organization's security awareness training program.
42. Provide guidance to the organization in order to improve the quality and control of information systems.
43. Evaluate potential opportunities and risks associated with emerging technologies, regulations, and industry practices.