Information Security Auditing Answer Key

Question	Correct Option
1	A
2	D
3	A
4	C
5	B
6	A
7	C
8	D
9	D
10	A
11	D
12	B
13	C
14	C
15	A
16	B
17	C
18	A
19	C
20	D
21	D
22	C
23	D
24	D
25	B
26	D
27	A
28	B
29	C
30	A

II		Attempt ***any one*** of the following:	6
	a	Explain traits of a successful Auditor. **ANSWER:** 1)Know the purpose of policies, standards, guidelines, and procedures. 2) Know the ISACA standards governing professional conduct and ethics: 3) Understand the general purpose of the audit and the role of the IS auditor. 4) Understand an audit role versus a nonaudit role. 5) Understand the importance of IS auditor independence. 6) Know the difference between discretionary and mandatory language.	

		7) Know the different types of audits. 8) Understand the need to protect audit documentation 9) Know how to use standard terms of reference. 10) Understand application of the evidence rule. 11) Understand the organizational structure.	
	b	Explain in detail purpose of Audits **ANSWER:** Audit objectives refer to the specific goals that must be accomplished by the audit. In contrast, a control objective refers to how an internal control should function. An audit generally incorporates several audit objectives. Audit objectives often focus on confirming that internal controls exist to minimize business risk and they function as expected. These audit objectives include assuring compliance with legal and regulatory requirements as well as the confidentiality, integrity, reliability and availability of Information and IT resources. Audit management may give an IS auditor a general control objective toreview and evaluate when performing an audit. A key element in planning an IS audit is to translate basic and wide-ranging audit objectives into specific IS audit objectives. For example, in a financial/operational audit, a control objective could be to ensure that transactions are properly posted to the general ledger accounts. However, in an IS audit, the objective could be extended to ensure that editing features are in place to detect errors in the coding of transactions that may impact the account-posting activities. An IS auditor must understand how general audit objectives can be translated into specific IS control objectives. Determining an audit's objectives is a critical step in planning an IS audit. One of the primary purposes of an IS audit is to identify control objectives and the related controls that address the objective. For example, an IS auditor's initial review of an information system should identify key controls. It should then be determined whether to test these controls for compliance. An IS auditor should identify both key general and application controls after developing an understanding and documenting the business processes and the applications/functions that support these processes and general support systems. Based on that understanding, an IS auditor should identify the key control points. Alternatively, an IS auditor may assist in assessing the integrity of financial reporting data, referred to as substantive testing, through CAATs.	
	c	What is Auditor Confidentiality? Explain in detail.	

		Answer: To ensure confidentiality, the auditor should adopt the following operating principles: Sensitive information is the property of the owner and should not be removed from the owner's office by the auditor. The auditor should contact legal counsel for advice concerning confidentiality and laws that would dictate disclosure to authorities. You should follow basic principles of confidentiality at all times. Many auditors use automated working papers (WPs) during an audit. Spreadsheets and report-writing templates are common tools to increase efficiency. We refer to audit checklists, procedures, computer-generated output, templates, and databases as working papers. The next level of automation is entering our workplace to aid even the smallest auditor. This includes more-advanced database automation, evidence tracking, and report-generation tools. The data must be protected with access control and regular data backup. Make sure to back up your work. It would be unforgivable to lose your audit work and client data by failing to implement your own recommended controls. Every auditor should seriously consider using locking security cables and privacy viewing screens for laptops. You will gain respect by demonstrating your concern for maintaining confidentiality while protecting assets. The laptop could still be stolen with broken parts lying on the floor, but at least you would have some evidence that the theft was not completely your fault. At prior audit firms where I worked, these controls were mandatory for continued employment. A document file archive is created during each audit. The archive is subject to laws governing records retention. Every auditor is advised to leave all records in the custody of the client unless criminal activity is suspected. The client shall maintain sole responsibility for the safe retention of the archive.	
2		**Attempt *<u>any one</u>* of the following:**	**6**
	a	Explain various Testing Methodologies used in system implementation. ANSWER: The following tests relate, to varying degrees, to the approaches that can be performed based on the size and complexity of the modified system: • Unit testing—The testing of an individual program or module. Unit testing uses a set of test cases that focus on the control structure of the procedural design. These tests ensure that the internal operation of the program performs according to specification.	

		• Interface or integration testing—A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit tested modules and build an integrated structure dictated by design. The term "integration testing" is also used to refer to tests that verify and validate the functioning of the application under test with other systems, in which a set of data is transferred from one system to another. • System testing—A series of tests designed to ensure that modified programs, objects, database schema, etc., which collectively constitute a new or modified system, function properly. These test procedures are often performed in a nonproduction test/development environment by software developers designated as a test team. The following specific analyses may be carried out during system testing: – Recovery testing—Checking the system's ability to recover after a software or hardware failure – Security testing —Making sure the modified/new system includes provisions for appropriate access controls and does not introduce any security holes that might compromise other systems – Load testing—Testing an application with large quantities of data to evaluate its performance during peak hours – Volume testing —Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records (data) the application can process – Stress testing—Studying the impact on the application by testing with an incremental number of concurrent users/services on the application to determine the maximum number of concurrent users/services the application can process – Performance testing —Comparing the system's performance to other equivalent systems using well defined benchmarks.	
	b	Explain Information Systems Acquisition and Development. ANSWER: For an IS auditor to provide assurance that an organization's objectives are being met by the management practices of its information systems, it is important that the IS auditor understand how an organization evaluates, develops, implements, maintains and disposes of its information systems and related components. A CISA candidate should have a sound understanding of the information systems (hardware	

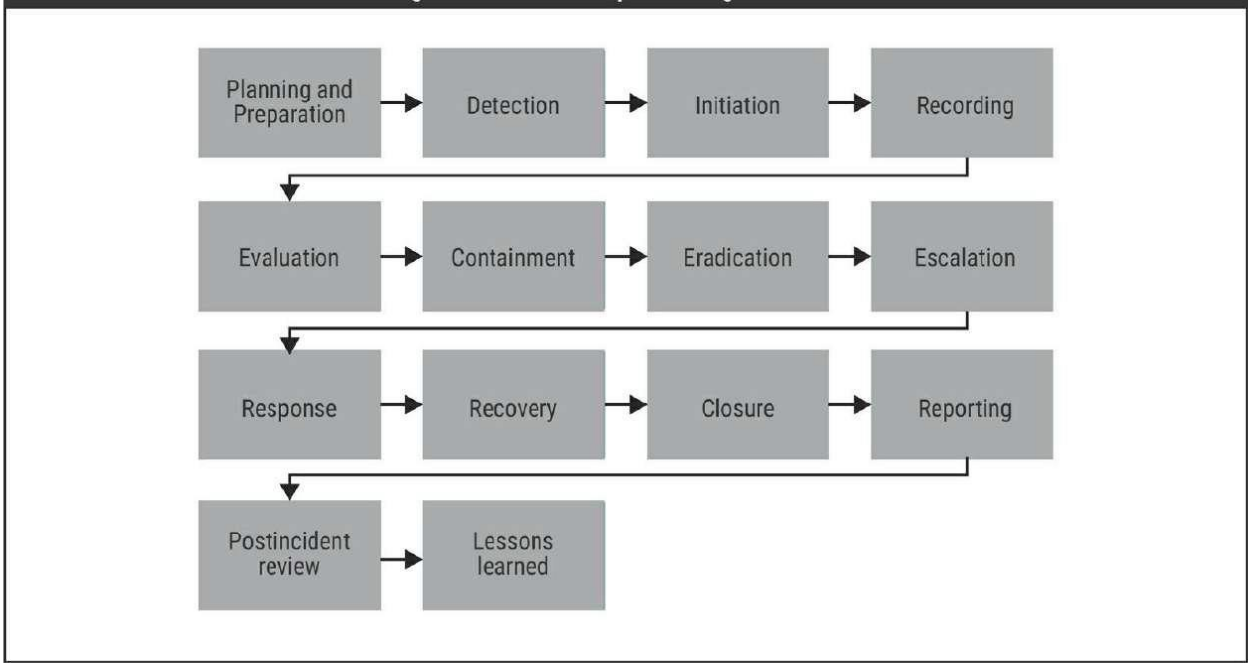
		and software) acquisition, development and implementation process. This understanding should extend beyond a definitional knowledge of terms and concepts and include an ability to identify vulnerabilities and risk and recommend appropriate controls to effectively mitigate risk. A thorough understanding of the phases of project management is also required. In addition, a CISA candidate should have a good understanding of various application systems andarchitectures, and the related processes, risk and controls.	
	c	Explain Configuration and Release Management. ANSWER: The effective and efficient development and maintenance of complicated IT systems requires that rigorous configuration, change and release management processes be implemented and adhered to within an organization. These processes provide systematic, consistent and unambiguous control on attributes of IT components comprising the system (hardware, software, firmware, and network connectivity including physical connecting media wire, fiber and radio frequency [RF]). Knowledge of the configuration status of computing environments is critical to system reliability, availability and security along with achieving timely maintenance of these systems. Changes to IT systems must be carefully assessed, planned, tested, approved, documented and communicated to minimize any undesirable consequences to the business processes. Configuration management tools will support change management and release management through the: 1.Identification of items affected by a proposed change to assist with impact assessment (functional, operational and security) 2. Recording configuration items affected by authorized changes 3. Implementation of changes in accordance with authorization records 4. Registering of configuration item changes when authorized changes and releases are implemented 5. Recording of baselines that are related to releases (with known consequences) to which an organization would revert if an implemented change fails 6. Preparing a release to avoid human errors and resource costs.	
3	**Attempt *<u>any one</u>* of the following:**		**6**
	a	Explain various technology component in IT service management. ANSWER: COMMON TECHNOLOGY COMPONENTS are	

		• Technology components • Hardware platforms • Basic concepts of, and history behind, the different types of computers • Advances in IT. (Elaboration required by students)	
	b	What is meant by Business Resilience and Business Impact Analysis. ANSWER: Business resilience describes an organization's ability to adapt to disruptions and incidents in order to maintain continuous operations and to protect the organization's assets. Most organizations have some degree of DRPs in place for the recovery of IT infrastructure, critical systems and associated data. However, many organizations have not taken the next step and developed plans for how key business units will function during a period of IT disruption. CISA candidates should be aware of the components of disaster recovery and business continuity plans, the importance of aligning one with the other, and aligning DRPs and business continuity plans (BCPs) with the organization's goals and risk tolerance. Also of importance are data backup, storage and retention and restoration. Business impact analysis (BIA) is a critical step in developing the business continuity strategy and the subsequent implementation of the risk countermeasures and the BCP in particular. BIA is used to evaluate the critical processes (and IT components supporting them) and to determine time frames, priorities, resources and interdependencies. Even if an extensive risk assessment was done prior to BIA, and the criticality and risk are input into BIA, the rule of thumb is to double-check. Often, the BIA uncovers some less visible, but nonetheless vital, component that supports the critical business process. Where IT activities have been outsourced to third-party service providers, the contractual commitments (in a BCP context) should also be considered. To perform this phase successfully, one should obtain an understanding of the organization, key business processes and IT resources used by the organization to support the key business processes. Often, this may be obtained from the risk assessment results. BIA requires a high level of senior management support/sponsorship and extensive involvement of IT and end-user personnel. The criticality of the information resources (e.g., applications, data, networks, system software, facilities) that support an organization's business processes must be approved by senior management. For the BIA, it is important to include all types of information resources and to look beyond traditional information resources (i.e., database servers).Information systems consist of multiple components. Some of the components (e.g., database servers or storage	

		arrays) are quite visible. Other components (e.g., gateways, transport servers, are collected for the BIA from different parts of the organization that own critical processes/applications. To evaluate the impact of downtime for a particular process/application, the impact bands are developed (i.e., high, medium, low) and, for each process, the impact is estimated in time (hours, days, weeks). The same approach is used when estimating the impact of data loss. If necessary, the financial impact may be estimated using the same techniques, assigning the financial value to the particular impact band.	
	c	Explain steps to create a Disaster Recovery Plans. ANSWER: As part of a greater business continuity planning process, IT disaster recovery planning follows the same path. After conducting a BIA and risk assessment (or determining the risk and effectiveness of mitigation controls otherwise), the IT disaster recovery strategy is developed. Implementing this strategy means making changes to: • IT systems • Networks • IT processing sites • Organization structure (headcount, roles, positions) • IT processes and procedures An IT DRP is a well-structured collection of processes and procedures intended to make the disaster response and recovery effort swift, efficient and effective to achieve the synergy between recovery teams. The plan should be documented and written in simple language that is understandable to all.	
4	**Attempt *<u>any one</u>* of the following:**		**6**
	a	Explain various IT standards and IT policies used in System implementation. ANSWER IT Policies Executive management and IT management are responsible for developing and issuing policies that support agreed-upon information technology objectives. Examples include a corporate acceptable use policy (AUP), antivirus protection policy, and the designation of information technology as the official custodian for corporate data. IT Standards Operating standards are developed from ISO standards, adapted by managers, and	

		then approved for use by executive management. One such standard is the separation of duties. Other examples include the hours of system availability and ensuring system certification by in-depth configuration testing prior to production use.	
	b	Explain System Development Lifecycle in detail. The Software Development Life Cycle (SDLC) refers to a methodology with clearly defined processes for creating high-quality software. in detail, the SDLC methodology focuses on the following phases of software development: • Requirement analysis • Planning • Software design such as architectural design • Software development • Testing • Deployment Elaborate answer required.	
	c	Explain Incident Handling Process in detail. ANSWER: Incident-Handling Process Incident response teams (IRTs) are structured into one of three categories: ■ Centralized team ■ Distributed team reporting to a central authority ■ Coordination team providing guidance and advice to individual responders Members of the IRT should be formally designated via a written charter. This will help eliminate disputes over members responding versus continuing to work on the tasks of their normal jobs. The staff of the IRT could be employees, outsourced, or a hybrid model. Team members may be needed 24/7, which creates a need for schedule planning. Each response will follow four phases of the incident response life cycle: Phase 1: Preparation Phase 2: Detection and Analysis Phase 3: Containment, Eradication, and Recovery Phase 4: Post-Incident Activity	

5		**Attempt *<u>any one</u>* of the following:**	**6**
	a	Explain the 5 phases of business continuity plan in detail. ANSWER: The 5 phases are given below Phase 1: Setting Up the BC Program Phase 2: The Discovery Process Phase 3: Plan Development Phase 4: Plan Implementation Phase 5: Maintenance and Integration (Detailed explanation required)	
	b	Explain the Role of IS Auditor in Disaster Recovery Plans. ANSWER: The auditor can use the following points for evaluation: ■ Compare the results of the business impact and risk analysis to the various strategies selected for each activity in the overall process timeline. Do the BIA research and workflowbased risk assessment support management's strategy? ■ Time delays are an absolute killer of business continuity plans. Has the client done a good job of documenting the recovery time objectives (RTOs)? Are the RTOs well founded and realistic? Does the organization have the hardware and skills necessary to recover data in sufficient time to meet each RTO? ■ Ask whether the organization's document outlines a 0 - to 100 - hour timeline.This type of timeline sequences and prioritizes the recovery by using RT, RP, RTO, RPO, LWIP, RWIP, SDO, and RO. The presence of this document is a powerful statement in favor of the client. Absence of this document foretells a questionable future. ■ Work backlogs exist every day in business. How does the organization intend to handle the backlog when the processing capability is significantly diminished? Manual methods are usually proposed because of the low cost; however, substantial testing would be required to prove that the organization could manually keep up with the volume of work. ■ An audit of the vital records inventory will tell an interesting story. Well - organized vital records foretell the future of a successful recovery. ■ When was the most recent training exercise? It would be valuable to review the exercise plan, the results, and the schedule of future exercises. Plans must be	

		exercised regularly to remain effective.	
	c	What is meant by Incident Response Management? Explain in detail. ANSWER: **Figure 5.37—Incident Response Management Phases**  Explanation is required.	