Certified Information Systems Auditor
CISA

QUESTION 1

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST

A. perform a business impact analysis (BIA).

B. issue an intermediate report to management.

C. evaluate the impact on current disaster recovery capability.

D. conduct additional compliance testing.

Answer: C Explanation

The first step that an IS auditor should take when finding that a business impact analysis (BIA) has not been performed is to evaluate the impact on current disaster recovery capability. A BIA is a process that identifies and analyzes the potential effects of disruptions to critical business functions and processes. A BIA helps determine the recovery priorities, objectives, and strategies for the organization. Without a BIA, the disaster recovery plan may not be aligned with the business needs and expectations, and may not provide adequate protection and recovery for the most critical assets and activities. Therefore, an IS auditor should assess how the lack of a BIA affects the current disaster recovery capability and identify any gaps or risks that need to be addressed.

Performing a BIA, issuing an intermediate report to management, and conducting additional compliance testing are not the first steps that an IS auditor should take when finding that a BIA has not been performed.

These steps may be done later in the audit process, after evaluating the impact on current disaster recovery capability. Performing a BIA is not the responsibility of the IS auditor, but of the business owners and managers. Issuing an intermediate report to management may be premature without sufficient evidence and analysis. Conducting additional compliance testing may not be relevant or necessary without a clear understanding of the disaster recovery requirements and objectives.

QUESTION 2

An organization's security policy mandates that all new employees must receive appropriate security awareness training. Which of the following metrics would BEST assure compliance with this policy?

A. Percentage of new hires that have completed the training.

B. Number of new hires who have violated enterprise security policies.

C. Number of reported incidents by new hires.

D. Percentage of new hires who report incidents

Answer: A Explanation

The best metric to assure compliance with the policy of providing security awareness training to all new employees is the percentage of new hires that have completed the training, as this directly measures the extent to which the policy is implemented and enforced. The number of new hires who have violated enterprise security policies, the number of reported incidents by new hires, and the percentage of new hires who report incidents are not directly related to the policy, as they may depend on other factors such as the nature and frequency of threats, the

effectiveness of security controls, and the reporting culture of the organization. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.7

QUESTION 3

Which of the following is the BEST data integrity check?

A. Counting the transactions processed per day

B. Performing a sequence check

C. Tracing data back to the point of origin

D. Preparing and running test data

Answer: C Explanation

Data integrity is the property that ensures that data is accurate, complete, consistent, and reliable throughout its lifecycle. The best data integrity check is tracing data back to the point of origin, which is the source where the data was originally created or captured. This check can verify that data has not been altered or corrupted during transmission, processing, or storage. It can also identify any errors or discrepancies in data entry or conversion. Counting the transactions processed per day is a performance measure that does not directly assess data integrity. Performing a sequence check is a validity check that ensures that data follows a predefined order or pattern. It can detect missing or out-of-order data elements, but it cannot verify their accuracy or completeness. Preparing and running test data is a testing technique that simulates real data to evaluate how a system handles different scenarios. It can help identify errors or bugs in the system logic or functionality, but it cannot ensure data integrity in production environments. References: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

QUESTION 4

An IS auditor is reviewing an organization's information asset management process. Which of the following would be of GREATEST concern to the auditor?

A. The process does not require specifying the physical locations of assets.

B. Process ownership has not been established.

C. The process does not include asset review.

D. Identification of asset value is not included in the process.

Answer: B Explanation

An IS auditor would be most concerned if process ownership has not been established for the information asset management process, as this would indicate a lack of accountability, responsibility, and authority for managing the assets throughout their lifecycle. The process owner should also ensure that the process is aligned with the organization's objectives, policies, and standards. The process should require specifying the physical locations of assets, include asset review, and identify asset value, but these are less critical than establishing process ownership. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

QUESTION 5

An IS auditor will be testing accounts payable controls by performing data analytics on the

entire population of transactions. Which of the following is MOST important for the auditor to confirm when sourcing the population data?

A. The data is taken directly from the system.

B. There is no privacy information in the data.

C. The data can be obtained in a timely manner.

D. The data analysis tools have been recently updated.

Answer: A Explanation

The most important thing for the auditor to confirm when sourcing the population data for testing accounts payable controls by performing data analytics is that the data is taken directly from the system. Taking the data directly from the system can help ensure that the data is authentic, complete, and accurate, and that it has not been manipulated or modified by any intermediary sources or processes. The other options are not as important as taking the data directly from the system, as they do not affect the validity or reliability of the data. There is no privacy information in the data is a privacy concern that can help protect the confidentiality and integrity of personal or sensitive data, but it does not affect the accuracy or completeness of the data. The data can be obtained in a timely manner is a logistical concern that can help facilitate the efficiency and effectiveness of the data analytics process, but it does not affect the authenticity or accuracy of the data. The data analysis tools have been recently updated is a technical concern that can help enhance the functionality and performance of the data analytics tools, but it does not affect the validity or reliability of the data.

References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

QUESTION 6

Which of the following is the BEST recommendation to prevent fraudulent electronic funds transfers by accounts payable employees?

A. Periodic vendor reviews

B. Dual control

C. Independent reconciliation

D. Re-keying of monetary amounts

E. Engage an external security incident response expert for incident handling.

Answer: B Explanation

The best recommendation to prevent fraudulent electronic funds transfers by accounts payable employees is dual control. Dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity. Dual control can prevent fraudulent electronic funds transfers by requiring independent verification and approval of payment requests, amounts, and recipients by different accounts payable employees. The other options are not as effective as dual control in preventing fraudulent electronic funds transfers, as they do not involve independent checks or approvals. Periodic vendor reviews are detective controls that can help identify any irregularities or anomalies in vendor payments, but they do not prevent fraudulent electronic funds transfers from occurring. Independent reconciliation is a detective control that can help compare and

confirm payment records with bank statements, but it does not prevent fraudulent electronic funds transfers from occurring. Re-keying of monetary amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent fraudulent electronic funds transfers from occurring. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

QUESTION 7

When determining whether a project in the design phase will meet organizational objectives, what is BEST to compare against the business case?

A. Implementation plan

B. Project budget provisions

C. Requirements analysis

D. Project plan

Answer: C

Explanation

Requirements analysis should be the best thing to compare against the business case when determining whether a project in the design phase will meet organizational objectives, because it defines the functional and non-functional specifications of the project deliverables that should satisfy the business needs and expectations. Requirements analysis can help evaluate whether the project design is aligned with the business case and whether it can achieve the desired outcomes and benefits. Implementation plan, project budget provisions, and project plan are also important aspects of a project in the design phase, but they are not as relevant as requirements analysis for comparing against the business case. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.1

QUESTION 8

During a new system implementation, an IS auditor has been assigned to review risk management at each milestone. The auditor finds that several risks to project benefits have not been addressed. Who should be accountable for managing these risks?

A. Enterprise risk manager

B. Project sponsor

C. Information security officer

D. Project manager

Answer: D Explanation

The project manager should be accountable for managing the risks to project benefits. Project benefits are the expected outcomes or value that a project delivers to its stakeholders, such as improved efficiency, quality, customer satisfaction, or revenue. Project risks are uncertain events or conditions that may affect the project objectives, scope, budget, schedule, or quality. The project manager is responsible for identifying, analyzing, prioritizing, responding to, and monitoring project risks throughout the project life cycle. The other options are not accountable for managing project risks, as they have different roles and responsibilities. The enterprise risk manager is responsible for overseeing the organization's overall risk management framework and strategy, but not for managing specific project risks. The project sponsor is responsible for initiating, approving, and supporting the project, but not