Isaca CISA Mock Exam

Shared by Lowery on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The business case for an information system investment should be available for review until the:

Options:

A- information system investment is retired.
B- information system has reached end of life.
C- formal investment decision is approved.
D- benefits have been fully realized.

Answer:

D

Explanation:

The business case for an information system investment is a document that provides the rationale and justification for the investment, based on the expected costs, benefits, risks, and impacts of the project12.The business case should be available for review until the benefits have been fully realized, because it serves as a baseline for measuring the actual performance and outcomes of the project against the planned ones34.This helps to evaluate the success and value of the investment, and to identify any gaps or issues that need to be addressed5.

Reference

1: The Business Case for Security - CISA

2: Beyond the Business Case: New Approaches to IT Investment

3: #HowTo: Build a Business Case for Cybersecurity Investment

4: ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB

5: The Business Case for Security | CISA

Question 2

Question Type: MultipleChoice

An organization has assigned two now IS auditors to audit a now system implementation. One of the auditors has an IT-related degree, and one has a business degree. Which ol the following is MOST important to meet the IS audit standard for proficiency?

Options:

A- The standard is met as long as one member has a globally recognized audit certification.
B- Technical co-sourcing must be used to help the new staff.
C- Team member assignments must be based on individual competencies.
D- The standard is met as long as a supervisor reviews the new auditors' work.

Answer:

C

Explanation:

Team member assignments based on individual competencies is the most important factor to meet the IS audit standard for proficiency. Proficiency is the ability to apply knowledge, skills and experience to perform audit tasks effectively and efficiently. The IS audit standard for proficiency requires that IS auditors must possess the knowledge, skills and discipline to perform audit tasks in accordance with applicable standards, guidelines and procedures. Team member assignments based on individual competencies is a way to ensure that each IS auditor is assigned to audit tasks that match their level of proficiency, and that the audit team as a whole has sufficient and appropriate proficiency to conduct the audit. The other options are not as important as option C, as they do not ensure that the IS auditors have the required proficiency to perform audit tasks. Having a globally recognized audit certification is a way to demonstrate proficiency in IS auditing, but it does not guarantee that the IS auditor has the specific knowledge, skills and experience needed for a particular audit task or system. Technical co-sourcing is a way to supplement the proficiency of the IS audit team by hiring external experts or consultants to perform certain audit tasks or functions, but it does not replace the need for internal IS auditors to have adequate proficiency. Having a supervisor review the new auditors' work is a way to ensure quality and accuracy of the audit work, but it does not ensure that the new auditors have the necessary proficiency to perform audit tasks independently or competently.Reference:CISA Review Manual (Digital Version) , Chapter 1: Information Systems Auditing Process, Section 1.4: Audit Skills and Competencies.

Question 3

Question Type: MultipleChoice

What is the MAIN purpose of an organization's internal IS audit function?

Options:

A- Identify and initiate necessary changes in the control environment to help ensure sustainable improvement.
B- Independently attest the organization's compliance with applicable legal and regulatory requirements.
C- Review the organization's policies and procedures against industry best practices and standards.
D- Provide assurance to management about the effectiveness of the organization's risk management and internal controls.

Answer:

D

Explanation:

Comprehensive and Detailed Step-by-Step

Theprimary roleof an internalIS audit functionis to provideindependent assuranceonrisk management, internal controls, and governance processes.

Option A (Incorrect):While audits may identifycontrol improvements, they donot initiate changes; management is responsible for implementation.

Option B (Incorrect):Compliance audits arepartof IS auditing, but the main focus isassurance on risk and controls, not just compliance.

Option C (Incorrect):Best practices and standards reviews are useful, but theydo not definethecore objectiveof an internal audit.

Option D (Correct):The internal audit function'smain goalis toassess and assurethe effectiveness of an organization'srisk management and internal controls.

Question 4

Question Type: MultipleChoice

Which of the following network communication protocols is used by network devices such as routers to send error messages and operational information indicating success or failure when

communicating with another IP address?

Options:

A- Transmission Control Protocol/Internet Protocol (TCP/IP)
B- Internet Control Message Protocol
C- Multipurpose Transaction Protocol
D- Point-to-Point Tunneling Protocol

Answer:

B

Question 5

Question Type: MultipleChoice

Which of the following is the main reason to involve IS auditors in the software acquisition process?

Options:

A- To help ensure hardware and operating system requirements are considered
B- To help ensure proposed contracts and service level agreements (SLAs) address key elements
C- To help ensure the project management process complies with policies and procedures
D- To help ensure adequate controls to address common threats and risks are considered

Answer:

A

Question 6

Question Type: MultipleChoice

A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is MOST relevant to creating the policy?

Options:

A- Business objectives
B- Business impact analysis (BIA)
C- Enterprise architecture (EA)
D- Recent incident trends

Answer:

A

Question 7

Question Type: MultipleChoice

An IS auditor observes that an organization's systems are being used for cryptocurrency mining on a regular basis. Which of the following is the auditor's FIRST course of action?

Options:

A- Report the incident immediately.
B- Recommend changing the organization's firewall settings.
C- Consult the organization's acceptable use policy.
D- Require mining software to be uninstalled.

Answer:

C

Question 8

Question Type: MultipleChoice

An IS auditor has been asked to advise on measures to improve IT governance within the organization. Which at the following is the BEST recommendation?

Options:

A- Implement key performance indicators (KPIs)
B- Implement annual third-party audits.

C- Benchmark organizational performance against industry peers.
D- Require executive management to draft IT strategy

Answer:

A

Explanation:

The best recommendation for improving IT governance within the organization is to implement key performance indicators (KPIs). KPIs are measurable values that show how effectively the organization is achieving its key business objectives.KPIs can help the organization tomonitor and evaluate the performance, efficiency, and alignment of its IT processes and resources with its business goals and strategies1.

The other options are not as effective as implementing KPIs for improving IT governance. Option B, implementing annual third-party audits, is a good practice but may not be sufficient or timely to identify and address the issues or gaps in IT governance. Option C, benchmarking organizational performance against industry peers, is a useful technique but may not reflect the specific needs and expectations of the organization's stakeholders. Option D, requiring executive management to draft IT strategy, is a necessary step but not enough to ensure that IT governance is implemented and monitored throughout the organization.

Question 9

Question Type: MultipleChoice

Which of the following would be MOST impacted if an IS auditor were to assist with the implementation of recommended control enhancements?

Options:

A- Independence
B- Integrity
C- Materiality
D- Accountability

Answer:

A

Explanation:

Independence would be most impacted if an IS auditor were to assist with the implementation of recommended control enhancements, as this would create a conflict of interest and impair the objectivity and credibility of the IS auditor. Integrity, materiality, and accountability are important attributes of an IS auditor, but they are not directly affected by the involvement in the implementation of control enhancements.Reference:CISA Review Manual (Digital Version), Chapter 1: Information Systems Auditing Process, Section 1.1: IS Audit Standards, Guidelines and Codes of Ethics

Question 10

Question Type: MultipleChoice

During an audit of an organization's risk management practices, an IS auditor finds several documented IT risk acceptances have not been renewed in a timely manner after the assigned expiration date When assessing the seventy of this finding, which mitigating factor would MOST significantly minimize the associated impact?

Options:

A- There are documented compensating controls over the business processes.
B- The risk acceptances were previously reviewed and approved by appropriate senior management
C- The business environment has not significantly changed since the risk acceptances were approved.
D- The risk acceptances with issues reflect a small percentage of the total population

Answer:

A

Explanation:

The mitigating factor that would most significantly minimize the impact of not renewing IT risk acceptances in a timely manner is having documented compensating controls over the business processes. Compensating controls are alternative controls that reduce or eliminate the risk when the primary control is not feasible or cost-effective. The other factors, such as previous approval by senior management, unchanged business environment, and small percentage of issues, do not mitigate the risk as effectively as compensating controls.Reference:ISACA CISA Review Manual 27th Edition Chapter 1