CISA$^{Q\&As}$

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

QUESTION 1

An IS auditor is reviewing an artificial intelligence (Al) and expert system application. The system has produced several critical errors with severe impact. Which of the following should the IS auditor do NEXT to understand the cause of the errors?

A. Review the decision-making logic built into the system.

B. Interview the system owner.

C. Understand the purpose and functionality of the system.

D. Verify system adherence to corporate policy.

Correct Answer: A

QUESTION 2

In which phase of the internal audit process is contact established with the individuals responsible for the business processes in scope for review?

A. Planning phase

B. Execution phase

C. Follow-up phase

D. Selection phase

Correct Answer: A

The planning phase is the stage of the internal audit process where contact is established with the individuals responsible for the business processes in scope for review. The planning phase involves defining the objectives, scope, and criteria of the audit, as well as identifying the key risks and controls related to the audited area. The planning phase also involves communicating with the auditee to obtain relevant information, documents, and data, as well as to schedule interviews, walkthroughs, and meetings. The planning phase aims to ensure that the audit team has a clear understanding of the audited area and its context, and that the audit plan is aligned with the expectations and needs of the auditee and other stakeholders. The execution phase is the stage of the internal audit process where the audit team performs the audit procedures according to the audit plan. The execution phase involves testing the design and operating effectiveness of the controls, collecting and analyzing evidence, documenting the audit work and results, and identifying any issues or findings. The execution phase aims to provide sufficient and appropriate evidence to support the audit conclusions and recommendations. The follow-up phase is the stage of the internal audit process where the audit team monitors and verifies the implementation of the corrective actions agreed upon by the auditee in response to the audit findings. The follow-up phase involves reviewing the evidence provided by the auditee, conducting additional tests or interviews if necessary, and evaluating whether the corrective actions have adequately addressed the root causes of the findings. The follow-up phase aims to ensure that the auditee has taken timely and effective actions to improve its processes and controls. The selection phase is not a standard stage of the internal audit process, but it may refer to the process of selecting which areas or functions to audit based on a risk assessment or an annual audit plan. The selection phase involves evaluating the inherent and residual risks of each potential auditable area, considering the impact, likelihood, and frequency of those risks, as well as other factors such as regulatory requirements, stakeholder expectations, previous audit results, and available resources. The selection phase aims to prioritize and allocate the audit resources to those areas that present the highest risks or opportunities for improvement. Therefore, option A is the correct answer. References: Stages and phases of internal audit - piranirisk.com Step-by-Step Internal Audit Checklist |

AuditBoard Audit Process | The Office of Internal Audit - University of Oregon

QUESTION 3

Which of the following is the BEST way to confirm that a digital signature is valid?

A. Confirm that the sender\\'s public key certificate is from a trusted certificate authority (CA).

B. Compare the hash value of the digital signature manually

C. Verify the digital signature by obtaining the senders public key

D. Request a valid private key from the sender and compare it with the public key

Correct Answer: A

QUESTION 4

Which of the following findings would be of MOST concern to an IS auditor performing a review of an end-user developed application that generates financial statements?

A. The application is not sufficiently supported by the IT department

B. There is not adequate training in the use of the application

C. There is no adequate user license for the application

D. There is no control to ensure accuracy of the processed data

Correct Answer: D

QUESTION 5

The MOST significant reason for using key performance indicators (KPIs) to track the progress of IT projects against initial targets is that they:

A. influence management decisions to outsource IT projects

B. identify which projects may require additional funding

C. provide timely indication of when corrective actions need to be taken

D. identify instances where increased stakeholder engagement is required

Correct Answer: D

QUESTION 6

While planning a security audit, an IS auditor is made aware of a security review carried out by external consultants. It is

MOST important for the auditor to:

A. re-perform the security review.

B. accept the findings and conclusions of the consultants.

C. review similar reports issued by the consultants.

D. assess the objectivity and competence of the consultants.

Correct Answer: D

QUESTION 7

When following up on a data breach, an IS auditor finds a system administrator may have compromised the chain of custody. Which of the following should the system administrator have done FIRST to preserve the evidence?

A. Perform forensic discovery

B. Notify key stakeholders

C. Quarantine the system

D. Notify the incident response team

Correct Answer: C

QUESTION 8

Which of the following is a social engineering attack method?

A. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone.

B. A hacker walks around an office building using scanning tools to search for a wireless network to gain access.

C. An intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties.

D. An unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door.

Correct Answer: A

Social engineering is a technique that exploits human weaknesses, such as trust, curiosity, or greed, to obtain information or access from a target. An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone is an example of a social engineering attack method, as it involves manipulating the employee into divulging sensitive information that can be used to compromise the network or system. A hacker walks around an office building using scanning tools to search for a wireless network to gain access, an intruder eavesdrops and collects sensitive information flowing through the network and sells it to third parties, and an unauthorized person attempts to gain access to secure premises by following an authorized person through a secure door are not examples of social engineering attack methods, as they do not involve human interaction or deception.
References: [ISACA CISA Review Manual 27th Edition], page 361.

QUESTION 9

A vendor requires privileged access to a key business application. Which of the following is the BEST recommendation to reduce the risk of data leakage?

A. Implement real-time activity monitoring for privileged roles

B. Include the right-to-audit in the vendor contract

C. Perform a review of privileged roles and responsibilities

D. Require the vendor to implement job rotation for privileged roles

Correct Answer: A

A vendor requires privileged access to a key business application. The best recommendation to reduce the risk of data leakage is to implement real-time activity monitoring for privileged roles. This is because real-time activity monitoring can provide visibility and accountability for the actions performed by the vendor with privileged access, such as creating, modifying, deleting, or copying data. Real-time activity monitoring can also enable timely detection and response to any unauthorized or suspicious activities that may indicate data leakage. Including the right-to-audit in the vendor contract is a good practice, but it may not be sufficient to prevent or detect data leakage in a timely manner, as audits are usually performed periodically or on-demand. Performing a review of privileged roles and responsibilities is also a good practice, but it may not address the specific risk of data leakage by the vendor with privileged access. Requiring the vendor to implement job rotation for privileged roles may reduce the risk of collusion or fraud, but it may not prevent or detect data leakage by any individual with privileged access. References: CISA Review Manual (Digital Version), [ISACA Privacy Principles and Program Management Guide]

QUESTION 10

The practice of periodic secure code reviews is which type of control?

A. Preventive

B. Compensating

C. Corrective

D. Detective

Correct Answer: A

QUESTION 11

During the discussion of a draft audit report. IT management provided suitable evidence fiat a process has been implemented for a control that had been concluded by the IS auditor as Ineffective. Which of the following is the auditor\\'s BEST action?

A. Explain to IT management that the new control will be evaluated during follow-up

B. Re-perform the audit before changing the conclusion.

C. Change the conclusion based on evidence provided by IT management.

D. Add comments about the action taken by IT management in the report.

Correct Answer: B

The auditor\\'s best action when IT management provides suitable evidence for a control that had been concluded as ineffective is to re-perform the audit before changing the conclusion. This means that the auditor should verify the validity, completeness, and timeliness of the evidence provided by IT management and test the effectiveness of the new control in meeting the audit objectives. The auditor should not change the conclusion based on evidence provided by IT management without re- performing the audit, as this could compromise the auditor\\'s independence and objectivity. The auditor should also not explain to IT management that the new control will be evaluated during follow-up or add comments about the action taken by IT management in the report, as these actions do not address the original audit finding. References: CISA Review Manual, 27th Edition, page 439

QUESTION 12

Which of the following is the GREATEST benefit of utilizing data analytics?

A. Improved communication with management due to more confidence with data results

B. Better risk assessments due to the identification of anomalies and trends

C. Higher-quality audit evidence due to more representative audit sampling

D. Expedient audit planning due to early identification of problem areas and incomplete data

Correct Answer: B

QUESTION 13

Which of the following should be the FIRST step in the incident response process for a suspected breach?

A. Inform potentially affected customers of the security breach

B. Notify business management of the security breach.

C. Research the validity of the alerted breach

D. Engage a third party to independently evaluate the alerted breach.

Correct Answer: C

The first step in the incident response process for a suspected breach is to research the validity of the alerted breach. An incident response process is a set of procedures that defines how to handle security incidents in a timely and effective manner. The first step in this process is to research the validity of the alerted breach, which means to verify whether the alert is genuine or false positive, to determine the scope and impact of the incident, and to gather relevant information for further analysis and action. Informing potentially affected customers of the security breach, notifying business management of the security breach, and engaging a third party to independently evaluate the alerted breach are also steps in the

incident response process, but they are not the first step.

References:

CISA Review Manual, 27th Edition, page 4251

CISA Review Questions, Answers and Explanations Database - 12 Month Subscription

QUESTION 14

An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would BEST help to reduce the risk of data leakage?

A. Requiring policy acknowledgment and nondisclosure agreements signed by employees

B. Providing education and guidelines to employees on use of social networking sites

C. Establishing strong access controls on confidential data

D. Monitoring employees\\' social networking usage

Correct Answer: B

While all the options can help reduce the risk of data leakage, providing education and guidelines to employees on the use of social networking sites would be the most effective. This is because it directly addresses the issue at hand - the use

of social networking sites for business purposes. Education and guidelines can help employees understand the risks associated with social media use and teach them how to safely and responsibly use these platforms for business purposes.

This includes understanding privacy settings, recognizing phishing attempts, and knowing what information should not be shared on these platforms.

References:

10 Social Media Guidelines for Employees in 2023 - Hootsuite

QUESTION 15

When an IS audit reveals that a firewall was unable to recognize a number of attack attempts, the auditor\\'s BEST recommendation is to place an intrusion detection system (IDS) between the firewall and:

A. the organization\\'s web server.

B. the demilitarized zone (DMZ).

C. the organization\\'s network.

D. the Internet

Correct Answer: D

The best recommendation is to place an intrusion detection system (IDS) between the firewall and the Internet. An IDS is a device or software that monitors network traffic for malicious activity and alerts the network administrator or takes preventive action. By placing an IDS between the firewall and the Internet, the IS auditor can enhance the security of the network perimeter and detect any attack attempts that the firewall was unable to recognize. The other options are not as effective as placing an IDS between the firewall and the Internet: Placing an IDS between the firewall and the organization\\'s web server would not protect the web server from external attacks that bypass the firewall. The web server should be placed in a demilitarized zone (DMZ), which is a separate network segment that isolates public-facing servers from the internal network. Placing an IDS between the firewall and the demilitarized zone (DMZ) would not protect the DMZ from external attacks that bypass the firewall. The DMZ should be protected by two firewalls, one facing the Internet and one facing the internal network, with an IDS monitoring both sides of each firewall. Placing an IDS between the firewall and the organization\\'s network would not protect the organization\\'s network from external attacks that bypass the firewall. The organization\\'s network should be protected by a firewall that blocks unauthorized traffic from entering or leaving the network, with an IDS monitoring both sides of the firewall.