Free Questions for CISA by go4braindumps

Shared by Quinn on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Which of the following should be an IS auditor's GREATEST concern when a data owner assigns an incorrect classification level to data?

Options:

A- Controls to adequately safeguard the data may not be applied.

B- Data may not be encrypted by the system administrator.

C- Competitors may be able to view the data.

D- Control costs may exceed the intrinsic value of the IT asset.

Answer:

A

Explanation:

According to the ISACA CISA Study Manual (2020), 'incorrectly classifying information or not implementing adequate controls to protect the information is a major risk' (p. 328). Therefore, the IS auditor's greatest concern should be that controls to adequately safeguard the data may not be applied.

Question 2

Which of the following is the MOST effective control to mitigate against the risk of inappropriate activity by employees?

Options:

A- User activity monitoring

B- Two-factor authentication

C- Network segmentation

D- Access recertification

Answer:

A

Explanation:

The most effective control to mitigate against the risk of inappropriate activity by employees is A. User activity monitoring. User activity monitoring (UAM) is a control that can be used to identify and monitor any suspicious or inappropriate user activity, such as unauthorized access or data manipulation. UAM can also be used to detect insider threats and detect any malicious activity that could lead to security breaches. Reference: ISACA CISA Study Manual, section 3.3.3.3.

Question 3

Question Type: MultipleChoice

An IS auditor evaluating the change management process must select a sample from the change log. What is the BEST way tor the auditor to confirm the change log is complete?

Options:

A- Interview change management personnel about completeness.

B- Take an item from the log and trace it back to the system.

C- Obtain management attestation of completeness.

D- Take the last change from the system and trace it back to the log.

Answer:

D

Explanation:

Taking the last change from the system and tracing it back to the log is the best way for the auditor to confirm the change log is complete, because:

It verifies that the most recent change made to the system is recorded and documented in the change log, which implies that the change log is up to date and accurate12.

It tests the effectiveness of the change management process and controls that ensure that all changes made to the system are authorized, approved, tested, implemented, and monitored123.

It provides evidence of the traceability and accountability of the change management process and personnel, which can help the auditor identify any gaps, errors, or risks in the process123.

Question 4

Question Type: **MultipleChoice**

Which of the following is the MOST efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves

for care?

Options:

A- Infrastructure as a Service (IaaS) provider

B- Software as a Service (SaaS) provider

C- Network segmentation

D- Dynamic localization

Answer:

B

Explanation:

The most efficient solution for a multi-location healthcare organization that wants to be able to access patient data wherever patients present themselves for care is B. Software as a Service (SaaS) provider. SaaS providers offer cloud-based services that allow organizations to access applications, data, and infrastructure on demand, making it easier to access patient data no matter where the patient is located. Reference: ISACA CISA Study Manual, section 5.3.3.1.

Question 5

Which of the following is MOST useful to an IS auditor performing a review of access controls for a document management system?

Options:

A- Policies and procedures for managing documents provided by department heads

B- A system-generated list of staff and their project assignments. roles, and responsibilities

C- Previous audit reports related to other departments' use of the same system

D- Information provided by the audit team lead an the authentication systems used by the department

Answer:

B

Explanation:

A system-generated list of staff and their project assignments, roles, and responsibilities is the most useful to an IS auditor performing a review of access controls for a document management system (DMS).A DMS is a system used to create, store, manage, and track electronic documents and images of paper-based documents through software1.Access controls are the mechanisms that regulate who can access, modify, or delete documents in a DMS, and under what conditions2.A system-generated list of staff and their project assignments, roles, and responsibilities helps the IS auditor to verify the appropriateness, accuracy, and completeness of the access rights granted to different users or groups of users in the DMS, based on the principle of least privilege and the segregation of duties23.

Policies and procedures for managing documents provided by department heads (A) are not the most useful to an IS auditor performing a review of access controls for a DMS.Policies and procedures are the documents that define the rules, standards, and guidelines for managing documents in a DMS, such as the document lifecycle, retention, classification, security, etc1. Policies and procedures are important to establish the expectations and requirements for document management, but they do not provide sufficient evidence or assurance of the actual implementation and effectiveness of the access controls in the DMS.

Previous audit reports related to other departments' use of the same system are not the most useful to an IS auditor performing a review of access controls for a DMS.Previous audit reports are the documents that summarize the findings, conclusions, and recommendations of previous audits conducted on the same or similar systems or processes4. Previous audit reports are useful to identify the common or recurring issues, risks, or gaps in the access controls of the DMS, as well as the best practices or lessons learned from other departments. However, previous audit reports do not reflect the current state or performance of the access controls in the DMS, and they may not be relevant or applicable to the specific department or scope of the current audit.

Information provided by the audit team lead on the authentication systems used by the department (D) are not the most useful to an IS auditor performing a review of access controls for a DMS.Authentication systems are the systems that verify the identity and credentials of the users who attempt to access the DMS, such as passwords, tokens, biometrics, etc2. Authentication systems are important to ensure the integrity and accountability of the users who access the DMS, but they do not provide sufficient information or assurance of the authorization and restriction of the users who access the DMS.Authorization and restriction are the aspects of access control that determine what actions or operations the users can perform on the documents in the DMS, such as read, write, edit, delete, etc2.

Question 6

Which of the following is MOST important to determine when conducting an audit Of an organization's data privacy practices?

Options:

A- Whether a disciplinary process is established for data privacy violations

B- Whether strong encryption algorithms are deployed for personal data protection

C- Whether privacy technologies are implemented for personal data protection

D- Whether the systems inventory containing personal data is maintained

Answer:

D

Explanation:

The systems inventory containing personal data is a crucial element for auditing an organization's data privacy practices.The systems inventory is a list of all the systems, applications, databases, and devices that collect, store, process, or transmit personal data within the organization12.The systems inventory helps the auditor to identify the scope, location, ownership, and classification of personal data, as well as the risks and controls associated with them12.The systems inventory also helps the auditor to verify compliance with data privacy laws, regulations, and internal policies that apply to different types of personal data

Question 7

Which of the following is the BEST indicator for measuring performance of IT help desk function?

Options:

A- Percentage of problems raised from incidents

B- Mean time to categorize tickets

C- Number 0t incidents reported

D- Number of reopened tickets

Answer:

D

Explanation:

The number of reopened tickets is a key performance indicator (KPI) that measures how often the IT help desk function fails to resolve the issues or problems reported by the customers on the first attempt123.A high number of reopened tickets indicates poor quality of service, low customer satisfaction, and wasted resources

Question 8

Which of the following be of GREATEST concern to an IS auditor reviewing on-site preventive maintenance for an organization's business-critical server hardware?

Options:

A- Preventive maintenance costs exceed the business allocated budget.

B- Preventive maintenance has not been approved by the information system

C- Preventive maintenance is outsourced to multiple vendors without requiring nondisclosure agreements (NDAs)

D- The preventive maintenance schedule is based on mean time between failures (MTBF) parameters.

Answer:

C

Explanation:

Having multiple vendors without NDAs can lead to unauthorized access to sensitive information, which could lead to a security breach. NDAs also help to ensure that the vendors are providing quality services and not cutting corners.

Question 9

A finance department has a multi-year project to upgrade the enterprise resource planning (ERP) system hosting the general ledger. and in year one, the system version upgrade will be applied. Which of the following should be the PRIMARY focus of the IS auditor reviewing the first year of the project?

Options:

A- unit testing

B- Network performance

C- User acceptance testing (UAT)

D- Regression testing

Answer:

D

Explanation:

Regression testing is a type of software testing that is used to verify that changes to a system or application do not introduce new bugs or cause existing features to break. It involves running tests to ensure that the system performs as expected after changes are applied.

Question 10

Question Type: **MultipleChoice**

The use of control totals satisfies which of the following control objectives?

Options:

A- Transaction integrity

B- Processing integrity

C- Distribution control

D- System recoverability

Answer:

B

Explanation:

Control totals are used to ensure that the processing of data is accurate and complete. This is done by comparing totals of records or transactions processed with the expected totals, which serves to ensure that the data is correctly processed and that any errors or discrepancies are detected.

To Get Premium Files for CISA Visit

For More Free Questions Visit

20% DISCOUNT