CISA Q&As

Certified Information Systems Auditor

Pass Isaca CISA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cisa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A manager Identifies active privileged accounts belonging to staff who have left the organization. Which of the following is the threat actor In this scenario?

A. Terminated staff

B. Unauthorized access

C. Deleted log data

D. Hacktivists

Correct Answer: A

A threat actor is an entity or individual that poses a potential harm or danger to an organization\\'s information systems or data. Terminated staff are the threat actors in this scenario, as they are former employees who may still have active privileged accounts that grant them access to sensitive or critical information or resources of the organization. Terminated staff may abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of the information systems or data, either intentionally or unintentionally. Unauthorized access is a threat event or action that occurs when an unauthorized entity or individual gains access to an organization\\'s information systems or data without permission or authorization. Unauthorized access is not a threat actor, but rather a result of a threat actor\\'s activity. Deleted log data is a threat consequence or impact that occurs when log data, which are records of events or activities that occur on an information system or network, are erased or corrupted by a threat actor. Deleted log data can affect the auditability, accountability, and visibility of the information system or network, and prevent detection or investigation of security incidents. Deleted log data is not a threat actor, but rather a result of a threat actor\\'s activity. Hacktivists are threat actors who use hacking techniques to promote a political or social cause or agenda. Hacktivists are not the threat actors in this scenario, as there is no indication that they are involved in this case.

QUESTION 2

Which of the following BEST protects an organization\\'s proprietary code during a joint- development activity involving a third party?

A. Statement of work (SOW)

B. Nondisclosure agreement (NDA)

C. Service level agreement (SLA)

D. Privacy agreement

Correct Answer: B

A nondisclosure agreement (NDA) is the best way to protect an organization\\'s proprietary code during a joint-development activity involving a third party. An NDA is a legal contract that binds the parties involved in a joint-development activity to keep confidential any information, data or materials that are shared or exchanged during the activity. An NDA specifies what constitutes confidential information, how it can be used, disclosed or protected, how long it remains confidential, what are the exceptions and remedies for breach of confidentiality, and other terms and conditions. An NDA can help to protect an organization\\'s proprietary code from being copied, modified, distributed or exploited by unauthorized parties without its consent or knowledge. The other options are not as effective as option B, as they do not address confidentiality issues specifically. A statement of work (SOW) is a document that defines the

scope, objectives, deliverables, tasks, roles, responsibilities, timelines and costs of a joint-development activity, but it does not cover confidentiality issues explicitly. A service level agreement (SLA) is a document that defines the quality, performance and availability standards and metrics for a service provided by one party to another party in a joint-development activity, but it does not cover confidentiality issues explicitly. A privacy agreement is a document that defines how personal information collected from customers or users is collected, used, disclosed and protected by one party or both parties in a joint-development activity, but it does not cover confidentiality issues related to proprietary code. References: CISA Review Manual (Digital Version) , Chapter 3: Information Systems Acquisition, Development and Implementation, Section 3.2: Project Management Practices.

QUESTION 3

Which of the following is the PRIMARY reason for an organization\\'s procurement processes to include an independent party who is not directly involved with business operations and related decision- making\\'?

A. To ensure continuity of processes and procedures

B. To optimize use of business team resources

C. To avoid conflicts of interest

D. To ensure favorable price negotiations

Correct Answer: C

QUESTION 4

The MOST effective method for an IS auditor to determine which controls are functioning in an operating system is to:

A. compare the current configuration to the corporate standard.

B. consult with the systems programmer.

C. consult with the vendor of the system.

D. compare the current configuration to the default configuration.

Correct Answer: A

QUESTION 5

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

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

Correct Answer: D

The answer D is correct because the most important thing to determine when conducting an audit of an organization\\'s data privacy practices is whether the systems inventory containing personal data is maintained. A systems inventory is a list of all the systems, applications, databases, and devices that store, process, or transmit personal data within the organization. Maintaining a systems inventory is essential for data privacy because it helps the organization to identify, classify, and protect the personal data it holds, as well as to comply with the relevant privacy laws and regulations. A systems inventory also enables the organization to perform data protection impact assessments (DPIAs), data breach notifications, data subject access requests, and data retention and disposal policies. The other options are not as important as option D. Whether a disciplinary process is established for data privacy violations (option A) is a policy issue that may deter or sanction the employees who violate the data privacy rules, but it does not directly affect the data privacy practices of the organization. Whether strong encryption algorithms are deployed for personal data protection (option B) is a technical issue that may enhance the security and confidentiality of the personal data, but it does not address the other aspects of data privacy, such as accuracy, consent, and purpose limitation. Whether privacy technologies are implemented for personal data protection (option C) is also a technical issue that may support the data privacy practices of the organization, but it does not guarantee that the organization follows the best practices or complies with the applicable laws and regulations. References: IS Audit Basics: Auditing Data Privacy Best Practices for Privacy Audits ISACA Produces New Audit and Assurance Programs for Data Privacy and Mobile Computing