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

Which of the following would provide the MOST important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

A. Findings from prior audits

B. Results of a risk assessment

C. An inventory of personal devices to be connected to the corporate network

D. Policies including BYOD acceptable user statements

Correct Answer: D

The most important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program is policies including BYOD acceptable user statements. Policies are documents that define the organization\\'s objectives, requirements, expectations, and responsibilities regarding a specific topic or area. BYOD policies should include acceptable user statements that specify what types of personal devices are allowed to connect to the corporate network, what security measures must be implemented on those devices, what data can be accessed or stored on those devices, what actions must be taken in case of device loss or theft, and what consequences will apply for noncompliance. Policies including BYOD acceptable user statements can provide an IS auditor with a clear understanding of the scope, criteria, and objectives of the BYOD program audit. Findings from prior audits, results of a risk assessment, and an inventory of personal devices to be connected to the corporate network are also useful inputs for planning a BYOD program audit, but they are not as important as policies including BYOD acceptable user statements. References: ISACA CISA Review Manual 27th Edition, page 381.

QUESTION 2

Which of the following is the GREATEST benefit of adopting an Agile audit methodology?

A. Better ability to address key risks

B. Less frequent client interaction

C. Annual cost savings

D. Reduced documentation requirements

Correct Answer: A

QUESTION 3

An IS auditor reviewing a job scheduling tool notices performance and reliability problems. Which of the following is MOST likely affecting the tool?

A. Administrator passwords do not meet organizational security and complexity requirements.

B. The number of support staff responsible for job scheduling has been reduced.

C. The scheduling tool was not classified as business-critical by the IT department.

D. Maintenance patches and the latest enhancement upgrades are missing.

Correct Answer: D

The performance and reliability of a job scheduling tool can be significantly affected if maintenance patches and the latest enhancement upgrades are missing. These patches and upgrades often contain fixes for known issues and improvements to the tool\\'s functionality. If they are not applied, the tool may continue to exhibit known problems or fail to benefit from enhancements that could improve its performance and reliability. While factors like administrator password requirements23, number of support staff45, and tool classification can impact various aspects of a tool\\'s operation, they are less likely to be the direct cause of performance and reliability problems. References: Patch Management Definition and Best Practices - Rapid7 Password must meet complexity requirements - Windows Security NIST\\'s New Password Rule Book: Updated Guidelines Offer Benefits and Risk - ISACA Workforce optimization: Staff scheduling with AI | McKinsey Poor Employee Scheduling - Major Consequences And Solutions A Critical Analysis of Job Shop Scheduling in Context of Industry 4.0

QUESTION 4

Which of the following is an IS auditor\\'s BEST recommendation to mitigate the risk of eavesdropping associated with an application programming interface (API) integration implementation?

A. Encrypt the extensible markup language (XML) file.

B. Implement Transport Layer Security (TLS).

C. Implement Simple Object Access Protocol (SOAP).

D. Mask the API endpoints.

Correct Answer: B

The best recommendation to mitigate the risk of eavesdropping associated with an API integration implementation is to implement Transport Layer Security (TLS). TLS is a cryptographic protocol that provides secure communication over a network by encrypting the data in transit and authenticating the parties involved. TLS can prevent unauthorized parties from intercepting, modifying or tampering with the data exchanged between the API endpoints. Encrypting the XML file, implementing SOAP, and masking the API endpoints are not sufficient to mitigate the risk of eavesdropping, as they do not provide end-to-end encryption or authentication for the API communication. References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

QUESTION 5

An internal review reveals an out-of-support human resources system. Which of the following is MOST important to determine when evaluating the associated risk?

A. Frequency of outages associated with the out-of-support system

B. The number of people accessing the out-of-support system

C. Exposure of the out-of-support system outside of the network

D. Timeline to replace the out-of-support system

Correct Answer: D

Latest CISA Dumps CISA VCE Dumps CISA Practice Test