Exam : **Cybersecurity-Audit-Certificate**

Title : ISACA Cybersecurity Audit Certificate Exam

Vendor : ISACA

Version : DEMO

NO.1 Which of the following is MOST critical to guiding and managing security activities throughout an organization to ensure objectives are met?

A. Allocating a significant amount of budget to security investments

B. Adopting industry security standards and frameworks

C. Establishing metrics to measure and monitor security performance

D. Conducting annual security awareness training for all employees

Answer: C

Explanation:

The MOST critical thing to guiding and managing security activities throughout an organization to ensure objectives are met is establishing metrics to measure and monitor security performance. This is because metrics provide quantifiable and objective data that can be used to evaluate the effectiveness and efficiency of security activities, as well as identify gaps and areas for improvement. Metrics also enable communication and reporting of security performance to stakeholders, such as senior management, board members, auditors, regulators, customers, etc. The other options are not as critical as establishing metrics, because they either involve spending money without knowing the return on investment (A), adopting standards without customizing them to fit the organization's context and needs (B), or conducting training without assessing its impact on behavior change (D).

NO.2 Which of the following contains the essential elements of effective processes and describes an improvement path considering quality and effectiveness?

A. Capability maturity model integration

B. Balanced scorecard

C. 60 270042009

D. COBIT 5

Answer: A

Explanation:

The document that contains the essential elements of effective processes and describes an improvement path considering quality and effectiveness is Capability Maturity Model Integration (CMMI). This is because CMMI is a framework that defines five levels of process maturity, from initial to optimized, and provides best practices and guidelines for improving the quality and effectiveness of processes across different domains, such as software development, service delivery, or cybersecurity. The other options are not documents that contain the essential elements of effective processes and describe an improvement path considering quality and effectiveness, but rather different types of documents or tools that provide guidance or recommendations for implementing policies or controls, such as Balanced Scorecard (B), ISO 27004:2009 C, or COBIT 5 (D).

NO.3 While risk is measured by potential activity, which of the following describes the actual occurrence of a threat?

A. Attack

B. Payload

C. Vulnerability

D. Target

Answer: A

Explanation:

An attack is the actual occurrence of a threat, which is a potential activity that could harm an asset. An attack is the result of a threat actor exploiting a vulnerability in a system or network to achieve a malicious objective. For example, a denial-of-service attack is the occurrence of a threat that aims to disrupt the availability of a service.

NO.4 Which of the following is the SLOWEST method of restoring data from backup media?

A. Monthly backup

B. Full backup

C. Differential Backup

D. Incremental backup

Answer: D

Explanation:

The SLOWEST method of restoring data from backup media is an incremental backup. This is because an incremental backup is a type of backup that only copies the files that have been created or modified since the previous backup, whether it was a full or an incremental backup. An incremental backup makes the restoration process slower, as it requires restoring multiple backups in a specific order and sequence, starting from the last full backup and then applying each incremental backup until the desired point in time is reached. The other options are not methods of restoring data from backup media that are slower than an incremental backup, but rather different types of backup procedures that copy files based on different criteria, such as monthly backup (A), full backup (B), or differential backup C.

NO.5 Which of the following security mechanisms provides the BEST protection of data when a computer is stolen?

A. Password-based access control

B. Digital signature

C. Secret key encryption

D. Cryptographic hash function

Answer: C

Explanation:

Secret key encryption, also known as symmetric encryption, involves a single key for both encryption and decryption. This method provides the best protection for data on a computer that is stolen because it renders the data unreadable without the key. Even if the thief has access to the physical hardware, without the secret key, the data remains secure and inaccessible.

NO.6 Which of the following mobile computing trends should cause the GREATEST concern for an organization that needs to protect sensitive organizational data?

A. Fluctuating size of form factors for mobile devices

B. Increasing amount of storage space available on mobile devices

C. Expanding availability of mobile network coverage

D. Growing consumer demand for advanced mobile technologies

Answer: B

Explanation:

The increasing amount of storage space available on mobile devices poses the greatest concern for organizations needing to protect sensitive data. Larger storage capacities allow for more data to be

stored on a device, which can include sensitive organizational information. If such a device is lost, stolen, or compromised, the potential for sensitive data to be accessed increases significantly. Additionally, the more data a device can hold, the more attractive it becomes as a target for attackers.
Reference = ISACA's resources highlight the risks associated with mobile devices' storage capabilities, especially when they contain sensitive organizational data. The threats, vulnerabilities, and risks related to the storage of sensitive data on mobile devices are discussed, emphasizing the importance of protecting such data from unauthorized access123.

NO.7 Which of the following is an important reason for tracing the access and origin of an intrusion once it has been detected?

A. To create appropriate security awareness content to avoid recurrence

B. To determine the impact of the intrusion event

C. To perform a root cause analysis of the intrusion event

D. To determine and correct any system weaknesses

Answer: C

Explanation:
Tracing the access and origin of an intrusion is crucial for performing a root cause analysis. This process involves identifying the underlying factors that led to the security breach. By understanding how the intrusion happened, organizations can better address the specific vulnerabilities that were exploited and implement more effective security measures to prevent similar incidents in the future.

NO.8 A healthcare organization recently acquired another firm that outsources its patient information processing to a third-party Software as a Service (SaaS) provider. From a regulatory perspective, which of the following is MOST important for the healthcare organization to determine?

A. Cybersecurity risk assessment methodology

B. Encryption algorithms used to encrypt the data

C. Incident escalation procedures

D. Physical location of the data

Answer: C

Explanation:
From a regulatory perspective, the MOST important thing for the healthcare organization to determine when outsourcing its patient information processing to a third-party Software as a Service (SaaS) provider is the incident escalation procedures. This is because incident escalation procedures define how security incidents involving patient information are reported, communicated, escalated, and resolved between the healthcare organization and the SaaS provider. This is essential for complying with regulatory requirements such as HIPAA, which mandate timely notification and response to breaches of protected health information. The other options are not as important as incident escalation procedures from a regulatory perspective, because they either relate to technical aspects that may not affect compliance (A, B), or operational aspects that may not affect patient information security (D).

NO.9 Which of the following is MOST important to verify when reviewing the effectiveness of an organization's identity management program?

A. Processes are approved by the process owner.

B. Processes are aligned with industry best practices.
C. Processes are centralized and standardized.
D. Processes are updated and documented annually.
Answer: B
Explanation:
The MOST important thing to verify when reviewing the effectiveness of an organization's identity management program is whether the processes are aligned with industry best practices. Identity management is the process of managing the identities and access rights of users across an organization's systems and resources. Industry best practices provide guidelines and standards for how to implement identity management in a secure, efficient, and compliant manner.

NO.10 What is the FIRST phase of the ISACA framework for auditors reviewing cryptographic environments?
A. Evaluation of implementation details
B. Hands-on testing
C. Hand-based shakeout
D. Inventory and discovery
Answer: D
Explanation:
The FIRST phase of the ISACA framework for auditors reviewing cryptographic environments is inventory and discovery. This is because the inventory and discovery phase helps auditors to identify and document the scope, objectives, and approach of the audit, as well as the cryptographic assets, systems, processes, and stakeholders involved in the cryptographic environment. The inventory and discovery phase also helps auditors to assess the maturity and effectiveness of the cryptographic governance and management within the organization. The other phases are not the first phase of the ISACA framework for auditors reviewing cryptographic environments, but rather follow after the inventory and discovery phase, such as evaluation of implementation details (A), hands-on testing (B), or risk-based shakeout C.

NO.11 Which of the following is commonly referred to as a Wi-Fi hotspot?
A. Local area network (LAN)
B. Wireless local area network (WLAN)
C. Wireless personal area network (WPAN)
D. Wide area network (WAN)
Answer: B
Explanation:
A Wi-Fi hotspot is a physical location where people can obtain Internet access, typically using Wi-Fi technology, via a wireless local area network (WLAN) using a router connected to an Internet service provider. Public hotspots are often found in places like coffee shops or hotels and are created from wireless access points configured to provide Internet access1.

NO.12 Why are security frameworks an important part of a cybersecurity strategy?
A. They serve to integrate and guide activities.
B. They contain the necessary policies and standards.

C. They provide protection to the organization.

D. They are required for regulatory compliance.

Answer: A

Explanation:

Security frameworks are crucial in a cybersecurity strategy because they provide a structured approach to managing and mitigating risks. They help in integrating various cybersecurity activities and guiding them towards achieving the strategic objectives of the organization. By establishing a common language and systematic methodology, they ensure that all parts of the organization's cybersecurity program are aligned and working cohesively.

NO.13 The most common use of asymmetric algorithms is to:

A. encrypt bulk data.

B. encrypt data streams.

C. distribute symmetric keys.

D. distribute asymmetric keys.

Answer: C

Explanation:

Asymmetric algorithms are commonly used to securely distribute symmetric keys. The asymmetric encryption process involves a public key for encryption and a private key for decryption. This method ensures that even if the public key is intercepted, the encrypted data cannot be decrypted without the corresponding private key. Symmetric keys are then used for the bulk encryption of data due to their efficiency in processing large volumes of information.

Reference = The use of asymmetric algorithms for key distribution is a well-established practice in the field of cryptography. It is mentioned in various ISACA resources that asymmetric encryption, such as RSA and ECC, is crucial for secure communications, especially for the initial exchange of symmetric keys, which are then used for encrypting data streams or bulk data123.

NO.14 A cloud service provider is used to perform analytics on an organization's sensitive dat a. A data leakage incident occurs in the service providers network from a regulatory perspective, who is responsible for the data breach?

A. The service provider

B. Dependent upon the nature of breath

C. Dependent upon specific regulatory requirements

D. The organization

Answer: D

Explanation:

A cloud service provider is used to perform analytics on an organization's sensitive data. A data leakage incident occurs in the service provider's network. From a regulatory perspective, the organization is responsible for the data breach. This is because the organization is the data owner and has the ultimate accountability and liability for the security and privacy of its data, regardless of where it is stored or processed. The organization cannot transfer or delegate its responsibility to the service provider, even if there is a contractual agreement or service level agreement that specifies the security obligations of the service provider. The other options are not correct, because they either imply that the service provider is responsible (A), or that the responsibility depends on the nature of breach (B) or specific regulatory requirements C, which are not relevant factors.