VirtuLearn

TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification preparation materials in the industry!

https://www.virtulearner.com
support@virtulearner.com

Isaca Cybersecurity-Audit-Certificate

ISACA Cybersecurity Audit Certificate Exam

QUESTION: 1
The second line of defense in cybersecurity includes:

A. conducting organization-wide control self-assessments.
B. risk management monitoring, and measurement of controls.
C. separate reporting to the audit committee within the organization.
D. performing attack and breach penetration testing.

Answer(s): B

Explanation:
The second line of defense in cybersecurity includes risk management monitoring, and measurement of controls. This is because the second line of defense is responsible for ensuring that the first line of defense (the operational managers and staff who own and manage risks) is effectively designed and operating as intended. The second line of defense also provides guidance, oversight, and challenge to the first line of defense. The other options are not part of the second line of defense, but rather belong to the first line of defense (A), the third line of defense C, or an external service provider (D).

QUESTION: 2
Within the NIST core cybersecurity framework, which function is associated with using organizational understanding to minimize risk to systems, assets, and data?

A. Detect
B. Identify
C. Recover
D. Respond

Answer(s): B

Explanation:
Within the NIST core cybersecurity framework, the identify function is associated with using organizational understanding to minimize risk to systems, assets, and data. This is because the identify function helps organizations to develop an organizational understanding of their cybersecurity risk management posture, as well as the threats, vulnerabilities, and impacts that could affect their business objectives. The other functions are not directly related to using organizational understanding, but rather focus on detecting (A), recovering C, or responding (D) to cybersecurity events.

QUESTION: 3
The "recover" function of the NISI cybersecurity framework is concerned with:

A. planning for resilience and timely repair of compromised capacities and service.
B. identifying critical data to be recovered m case of a security incident.
C. taking appropriate action to contain and eradicate a security incident.
D. allocating costs incurred as part of the implementation of cybersecurity measures.

Answer(s): A

Explanation:
The "recover" function of the NIST cybersecurity framework is concerned with planning for resilience and timely repair of compromised capacities and service. This is because the recover function helps organizations to restore normal operations as quickly as possible after a cybersecurity incident, while also learning from the incident and improving their security posture. The other options are not part of the recover function, but rather belong to the identify (B), respond C, or protect (D) functions.

QUESTION: 4
Availability can be protected through the use of:

A. user awareness training and related end-user training.
B. access controls. We permissions, and encryption.
C. logging, digital signatures, and write protection.
D. redundancy, backups, and business continuity management

Answer(s): D

Explanation:
Availability can be protected through the use of redundancy, backups, and business continuity management. This is because these measures help to ensure that systems, data, and services are accessible and functional at all times, even in the event of a disruption or disaster. The other options are not directly related to protecting availability, but rather focus on enhancing confidentiality (A), integrity C, or awareness (D).

QUESTION: 5
Which of the following would provide the BEST basis for allocating proportional protection activities when comprehensive classification is not feasible?

A. Single classification level allocation
B. Business process re-engineering
C. Business dependency assessment
D. Comprehensive cyber insurance procurement

Answer(s): C

Explanation:
The BEST basis for allocating proportional protection activities when comprehensive classification is not feasible is a business dependency assessment. This is because a business dependency assessment helps to identify the criticality and sensitivity of business processes and their supporting assets, based on their contribution to the organization's objectives and value proposition. This allows for prioritizing protection activities according to the level of risk and impact. The other options are not as effective as a business dependency assessment, because they either use a single classification level allocation (A), which does not account for different levels of risk and impact; require a significant amount of time and resources to perform a business process re-engineering (B); or rely on external parties to cover potential losses without reducing the likelihood or impact of incidents (D).

QUESTION: 6