# Free Questions for Cybersecurity-Audit-Certificate by go4braindumps

## Shared by Nunez on 29-01-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

What would be an IS auditor's BEST response to an IT managers statement that the risk associated with the use of mobile devices in an organizational setting is the same as for any other device?

## Options:

**A-** Replication of privileged access and the greater likelihood of physical loss increases risk levels.

**B-** The risk associated with mobile devices is less than that of other devices and systems.

**C-** The risk associated with mobile devices cannot be mitigated with similar controls for workstations.

**D-** The ability to wipe mobile devices and disable connectivity adequately mitigates additional

## Answer:

A

## Explanation:

The BEST response to an IT manager's statement that the risk associated with the use of mobile devices in an organizational setting is the same as for any other device is thatreplication of privileged access and the greater likelihood of physical loss increases risk levels.

Mobile devices pose unique risks to an organization due to their portability, connectivity, and functionality. Mobile devices may store or access sensitive data or systems that require privileged access, which can be compromised if the device is lost, stolen, or hacked. Mobile devices also have a higher chance of being misplaced or taken by unauthorized parties than other devices.

# Question 2

**Question Type:** MultipleChoice

Which of the following is a limitation of intrusion detection systems (IDS)?

## Options:

**A-** Limited evidence on intrusive activity

**B-** Application-level vulnerabilities

**C-** Lack of Interface with system tools

**D-** Weak passwords for the administration console

## Answer:

B

### Explanation:

A limitation of intrusion detection systems (IDS) is that they cannot detectapplication-level vulnerabilities. An IDS is a tool that monitors network traffic or system activity and alerts on any suspicious or malicious events. However, an IDS cannot analyze the logic or functionality of applications and identify vulnerabilities such as SQL injection, cross-site scripting, or broken authentication.

## Question 3

**Question Type:** MultipleChoice

Which of the following is an attack attribute of an advanced persistent threat (APT) that is designed to remove data from systems and networks?

### Options:

**A-** Adversarial threat event

**B-** Exfiltration attack vector

**C-** Infiltration attack vector

**D-** Kill chain modeling

### Answer:

B

### Explanation:

An example of an attack attribute of an advanced persistent threat (APT) that is designed to remove data from systems and networks is anexfiltration attack vector. An exfiltration attack vector is a method or channel that an APT uses to transfer data from a compromised system or network to an external location. Examples of exfiltration attack vectors include email, FTP, DNS, HTTP, or covert channels.

## Question 4

**Question Type:** MultipleChoice

Which control mechanism is used to detect the unauthorized modification of key configuration settings?

### Options:

**A-** Sandboxing

**B-** Whitelisting

**C-** URL filtering

**D-** File integrity

### Answer:

D

### Explanation:

The control mechanism that is used to detect the unauthorized modification of key configuration settings isfile integrity. File integrity is the property of ensuring that files are not altered or corrupted by unauthorized users or processes. File integrity can be monitored by using tools that compare the current state of files with a baseline or checksum and alert on any changes.

## Question 5

**Question Type:** MultipleChoice

Which of the following is an example of an application security control?

## Options:

**A-** Secure coding

**B-** User security awareness training

**C-** Security operations center

**D-** Intrusion detection

## Answer:

A

## Explanation:

An example of an application security control issecure coding. Secure coding is the practice of developing software applications that follow security principles and standards to prevent or mitigate common vulnerabilities and risks. Secure coding involves applying techniques such as input validation, output encoding, error handling, encryption, and testing.

# Question 6

**Question Type:** MultipleChoice

In public key cryptography, digital signatures are primarily used to;

## Options:

**A-** ensure message integrity.

**B-** ensure message accuracy.

**C-** prove sender authenticity.

**D-** maintain confidentiality.

## Answer:

C

## Explanation:

In public key cryptography, digital signatures are primarily used toprove sender authenticity. A digital signature is a cryptographic technique that allows the sender of a message to sign it with their private key, which can only be decrypted by their public key. The recipient can verify that the message was sent by the sender and not tampered with by using the sender's public key.

# Question 7

**Question Type:** MultipleChoice

While risk is measured by potential activity, which of the following describes the actual occurrence of a threat?

## Options:

**A-** Attack

**B-** Payload

**C-** Vulnerability

**D-** Target

## Answer:

A

## Explanation:

Anattackis 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.

# Question 8

**Question Type:** MultipleChoice

Which of the following is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability?

## Options:

**A-** Cross-site scripting vulnerability

**B-** SQL injection vulnerability

**C-** Memory leakage vulnerability

**D-** Zero-day vulnerability

## Answer:

D

## Explanation:

A computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability is a zero-day vulnerability. This is because a zero-day vulnerability is a type of vulnerability that has not been reported or disclosed to the public or to the software vendor yet, and may be exploited by attackers before it is patched or fixed. A zero-day vulnerability poses a high risk to systems and applications that are affected by it, as there may be no known defense or solution against it. The other options are not computer-software vulnerabilities that are unknown to those who would be interested in mitigating the vulnerability, but rather types of vulnerabilities that are known and reported to the public or to the software vendor, such as cross-site scripting vulnerability (A), SQL injection vulnerability (B), or memory leakage vulnerability .

# Question 9

**Question Type:** MultipleChoice

Which of the following is MOST important to ensure the successful implementation of continuous auditing?

## Options:

**A-** Budget for additional storage hardware

**B-** Budget for additional technical resources

**C-** Top management support

**D-** Surplus processing capacity

## Answer:

C

## Explanation:

The MOST important factor to ensure the successful implementation of continuous auditing is top management support. This is because top management support helps to provide the vision, direction, and resources for implementing continuous auditing within the organization. Top management support also helps to overcome any resistance or challenges that may arise from implementing continuous auditing, such as cultural change, stakeholder buy-in, process reengineering, etc. Top management support also helps to ensure that the results and findings of continuous auditing are communicated and acted upon by the relevant decision-makers and stakeholders. The other options are not factors that are more important than top management support for ensuring the successful implementation of continuous auditing, but rather different aspects or benefits of continuous auditing, such as storage hardware (A), technical resources (B), or processing capacity (D).

# Question 10

**Question Type:** MultipleChoice

Which of the following is the SLOWEST method of restoring data from backup media?

## Options:

**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 .

# Question 11

**Question Type:** MultipleChoice

What is the MAIN consideration when storing backup files?

## Options:

**A-** Utilizing solid slate device (SSDJ media for quick recovery

**B-** Storing backup files on public cloud storage

**C-** Protecting the off-site data backup copies from unauthorized access

**D-** Storing copies on-site for ease of access during incident response

## Answer:

C

## Explanation:

The MAIN consideration when storing backup files is protecting the off-site data backup copies from unauthorized access. This is because protecting the off-site data backup copies from unauthorized access helps to ensure the confidentiality and integrity of the backup data, and prevent any unauthorized or malicious disclosure, modification, or deletion of the backup data. Protecting the off-site data backup copies from unauthorized access also helps to comply with any regulatory or contractual requirements that may apply to the

backup data. The other options are not the main consideration when storing backup files, but rather different aspects or factors that affect the backup process, such as using solid state device (SSD) media (A), storing backup files on public cloud storage (B), or storing copies on-site (D).