Free Questions for CISM by certsdeals

Shared by Deleon on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager?

Options:

A- Managing the impact

B- Identifying unacceptable risk levels

C- Assessing vulnerabilities

D- Evaluating potential threats

Answer:

A

Explanation:

When preventive controls to appropriately mitigate risk are not feasible, the most important action for the information security manager is to manage the impact, which means taking measures to reduce the likelihood or severity of the consequences of the risk. Managing the impact can involve using alternative controls, such as engineering, administrative, or personal protective controls, that can lower the exposure or harm to the organization. The other options, such as identifying unacceptable risk levels, assessing vulnerabilities, or evaluating potential threats, are part of the risk assessment process, but they are not actions to mitigate risk when preventive controls are not feasible. Reference:

https://bcmmetrics.com/risk-mitigation-evaluating-your-controls/

https://www.osha.gov/safety-management/hazard-prevention

https://www.cdc.gov/niosh/topics/hierarchy/default.html

Question 2

Question Type: MultipleChoice

An information security manager has identified that privileged employee access requests to production servers are approved; but user actions are not logged. Which of the following should be the GREATEST concern with this situation?

Options:

A- Lack of availability

B- Lack of accountability

C- Improper authorization

D- Inadequate authentication

Answer:

B

Explanation:

The greatest concern with the situation of privileged employee access requests to production servers being approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. Reference:

https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-pam

https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices

https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

Question 3

Question Type: MultipleChoice

An incident response team has established that an application has been breached. Which of the following should be done NEXT?

Options:

A- Maintain the affected systems in a forensically acceptable state

B- Conduct a risk assessment on the affected application

C- Inform senior management of the breach.

D- Isolate the impacted systems from the rest of the network

Answer:

D

Explanation:

The next thing an incident response team should do after establishing that an application has been breached is to isolate the impacted systems from the rest of the network, which means disconnecting them from the internet or other network connections to prevent further

spread of the attack or data exfiltration. Isolating the impacted systems can help to contain the breach and limit its impact on the organization. The other options, such as maintaining the affected systems in a forensically acceptable state, conducting a risk assessment, or informing senior management, may be done later in the incident response process, after isolating the impacted systems.
Reference:

https://www.crowdstrike.com/cybersecurity-101/incident-response/

https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks

https://www.invicti.com/blog/web-security/incident-response-steps-web-application-security/

Question 4

Question Type: MultipleChoice

Which of the following MUST be established to maintain an effective information security governance framework?

Options:

A- Security controls automation

B- Defined security metrics

C- Change management processes

D- Security policy provisions

Answer:

D

Explanation:

Security policy provisions are the statements or rules that define the information security objectives, principles, roles and responsibilities, and requirements for the organization. Security policy provisions must be established to maintain an effective information security governance framework, as they provide the foundation and direction for the information security activities and processes within the organization. Security policy provisions also help to align the information security governance framework with the business strategy and objectives, and ensure compliance with relevant laws and regulations. The other options, such as security controls automation, defined security metrics, or change management processes, are important components of an information security governance framework, but they are not essential to establish it. Reference:

https://www.iso.org/standard/74046.html

https://www.nist.gov/cyberframework

https://www.iso.org/standard/27001

Question 5

Question Type: MultipleChoice

Which of the following should an information security manager do FIRST after learning through mass media of a data breach at the organization's hosted payroll service provider?

Options:

A- Suspend the data exchange with the provider

B- Notify appropriate regulatory authorities of the breach.

C- Initiate the business continuity plan (BCP)

D- Validate the breach with the provider

Answer:

D

Explanation:

The first thing an information security manager should do after learning through mass media of a data breach at the organization's hosted payroll service provider is to validate the breach with the provider, which means contacting the provider directly and confirming the details and scope of the breach, such as when it occurred, what data was compromised, and what actions the provider is taking to mitigate the impact. Validating the breach with the provider can help the information security manager assess the situation accurately and plan the next steps accordingly. The other options, such as suspending the data exchange, notifying regulatory authorities, or initiating the business continuity plan, may be premature or unnecessary before validating the breach with the provider. Reference:

https://www.wired.com/story/sequoia-hr-data-breach/

https://cybernews.com/news/kronos-major-hr-and-payroll-service-provider-hit-with-ransomware-warns-of-a-long-outage/

https://www.afr.com/work-and-careers/workplace/pay-in-crisis-as-major-payroll-company-hacked-20211117-p599mr

Question 6

Question Type: MultipleChoice

An employee of an organization has reported losing a smartphone that contains sensitive information The BEST step to address this situation is to:

Options:

A- disable the user's access to corporate resources.

B- terminate the device connectivity.

C- remotely wipe the device

D- escalate to the user's management

Answer:

C

Explanation:

The best step to address the situation of losing a smartphone that contains sensitive information is to remotely wipe the device, which means erasing all the data on the device and restoring it to factory settings. Remotely wiping the device can prevent unauthorized access to the sensitive information and protect the organization from data breaches or leaks. Remotely wiping the device can be done through services such as Find My Device for Android or Find My iPhone for iOS, or through mobile device management (MDM) solutions. The other options, such as disabling the user's access, terminating the device connectivity, or escalating to the user's management, may not be effective or timely enough to secure the sensitive information on the device. Reference:

https://www.security.org/resources/protect-data-lost-device/

https://support.google.com/android/answer/6160491?hl=en

https://www.pcmag.com/how-to/locate-lock-erase-how-to-find-lost-android-phone

Question 7

Question Type: MultipleChoice

A business requires a legacy version of an application to operate but the application cannot be patched. To limit the risk exposure to the business, a firewall is implemented in front of the legacy application. Which risk treatment option has been applied?

Options:

A- Mitigate

B- Accept

C- Transfer

D- Avoid

Answer:

A

Explanation:

Mitigate is the risk treatment option that has been applied by implementing a firewall in front of the legacy application because it helps to reduce the impact or probability of a risk. Mitigate is a process of taking actions to lessen the negative effects of a risk, such as implementing security controls, policies, or procedures. A firewall is a security device that monitors and filters the network traffic between the legacy application and the external network, blocking or allowing packets based on predefined rules. A firewall helps to mitigate the risk of unauthorized access, exploitation, or attack on the legacy application that cannot be patched. Therefore, mitigate is the correct answer.

https://simplicable.com/risk/risk-treatment

https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/

https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment.