Free Questions for CISSP by braindumpscollection

Shared by Reilly on 20-10-2022

For More Free Questions and Preparation Resources

Question 1

In setting expectations when reviewing the results of a security test, which of the following statements is MOST important to convey to reviewers?

Options:

A- The target's security posture cannot be further compromised.

B- The results of the tests represent a point-in-time assessment of the target(s).

C- The accuracy of testing results can be greatly improved if the target(s) are properly hardened.

D- The deficiencies identified can be corrected immediately

Answer:

C

Question 2

Which of the following is an important design feature for the outer door o f a mantrap?

Options:

A- Allow it to be opened by an alarmed emergency button.

B- Do not allow anyone to enter it alone.

C- Do not allow it to be observed by dosed-circuit television (CCTV) cameras.

D- Allow it be opened when the inner door of the mantrap is also open

Answer:

D

Question 3

Question Type: **MultipleChoice**

Which of the following BEST describes the use of network architecture in reducing corporate risks associated with mobile devices?

Options:

A- Maintaining a 'closed applications model on all mobile devices depends on demilitarized 2one (DM2) servers

B- Split tunneling enabled for mobile devices improves demilitarized zone (DMZ) security posture

C- Segmentation and demilitarized zone (DMZ) monitoring are implemented to secure a virtual private network (VPN) access for mobile devices

D- Applications that manage mobile devices are located in an Internet demilitarized zone (DMZ)

Answer:

C

Question 4

Question Type: **MultipleChoice**

Information Security Continuous Monitoring (1SCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management

decisions. Which of the following is the FIRST step in developing an ISCM strategy and implementing an ISCM program?

Options:

A- Define a strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

B- Conduct a vulnerability assessment to discover current threats against the environment and incorporate them into the program.

C- Respond to findings with technical management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

D- Analyze the data collected and report findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
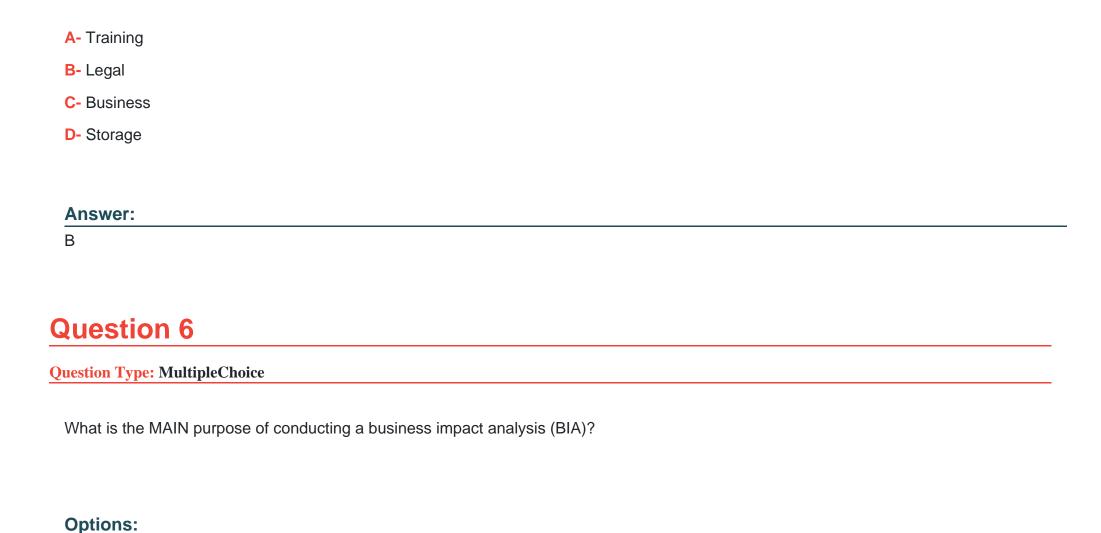
Answer:

A

Question 5

Question Type: MultipleChoice

Which of the following is the FIRST requirement a data owner should consider before implementing a data retention policy?

Options:

A- Training

B- Legal

C- Business

D- Storage

Answer:

B

Question 6

Question Type: MultipleChoice

What is the MAIN purpose of conducting a business impact analysis (BIA)?

Options:

A- To determine the critical resources required to recover from an incident within a specified time period

B- To determine the effect of mission-critical information system failures on core business processes

C- To determine the cost for restoration of damaged information system

D- To determine the controls required to return to business critical operations

Answer:

B

Question 7

Question Type: **MultipleChoice**

When designing a Cyber-Physical System (CPS), which of the following should be a security practitioner's first consideration?

Options:

A- Detection of sophisticated attackers

B- Resiliency of the system

C- Topology of the network used for the system

D- Risk assessment of the system

Answer:

B

Question 8

How does security in a distributed file system using mutual authentication differ from file security in a multi-user host?

Options:

A- Access control can rely on the Operating System (OS), but eavesdropping is

B- Access control cannot rely on the Operating System (OS), and eavesdropping

C- Access control can rely on the Operating System (OS), and eavesdropping is

D- Access control cannot rely on the Operating System (OS), and eavesdropping

Answer:

C

Question 9

Which of the following is the PRIMARY issue when analyzing detailed log information?

Options:

A- Logs may be unavailable when required

B- Timely review of the data is potentially difficult

C- Most systems and applications do not support logging

D- Logs do not provide sufficient details of system and individual activities

Answer:

D

Question 10

Question Type: **MultipleChoice**

Which of the following will accomplish Multi-Factor Authentication (MFA)?

Options:

A- Issuing a smart card with a user-selected Personal Identification Number (PIN)

B- Requiring users to enter a Personal Identification Number (PIN) and a password

C- Performing a palm and retinal scan

D- Issuing a smart card and a One Time Password (OTP) token

Answer:

A

Question 11

Question Type: MultipleChoice

Which of the following is a standard Access Control List (ACL) element that enables a router to filter Internet traffic?

Options:

A- Media Access Control (MAC) address

B- Internet Protocol (IP) address

C- Security roles

D- Device needs

Answer:

B

To Get Premium Files for CISSP Visit

https://www.p2pexams.com/products/cissp

For More Free Questions Visit

https://www.p2pexams.com/isc2/pdf/cissp

20% DISCOUNT