TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **CAS-002**

Title : CompTIA Advanced Security Practitioner (CASP)

Version : DEMO

1.An insurance company is looking to purchase a smaller company in another country. Which of the following tasks would the security administrator perform as part of the security due diligence?
A. Review switch and router configurations
B. Review the security policies and standards
C. Perform a network penetration test
D. Review the firewall rule set and IPS logs
Answer: B

2.A new piece of ransomware got installed on a company's backup server which encrypted the hard drives containing the OS and backup application configuration but did not affect the deduplication data hard drives. During the incident response, the company finds that all backup tapes for this server are also corrupt. Which of the following is the PRIMARY concern?
A. Determining how to install HIPS across all server platforms to prevent future incidents
B. Preventing the ransomware from re-infecting the server upon restore
C. Validating the integrity of the deduplicated data
D. Restoring the data will be difficult without the application configuration
Answer: D

3.The Chief Executive Officer (CEO) of a large prestigious enterprise has decided to reduce business costs by outsourcing to a third party company in another country. Functions to be outsourced include: business analysts, testing, software development and back office functions that deal with the processing of customer data. The Chief Risk Officer (CRO) is concerned about the outsourcing plans. Which of the following risks are MOST likely to occur if adequate controls are not implemented?
A. Geographical regulation issues, loss of intellectual property and interoperability agreement issues
B. Improper handling of client data, interoperability agreement issues and regulatory issues
C. Cultural differences, increased cost of doing business and divestiture issues
D. Improper handling of customer data, loss of intellectual property and reputation damage
Answer: D

4.A security analyst has been asked to develop a quantitative risk analysis and risk assessment for the company's online shopping application. Based on heuristic information from the Security Operations Center (SOC), a Denial of Service Attack (DoS) has been successfully executed 5 times a year. The Business Operations department has determined the loss associated to each attack is $40,000. After implementing application caching, the number of DoS attacks was reduced to one time a year. The cost of the countermeasures was $100,000. Which of the following is the monetary value earned during the first year of operation?
A. $60,000
B. $100,000
C. $140,000
D. $200,000
Answer: A

5.The Information Security Officer (ISO) is reviewing new policies that have been recently made effective and now apply to the company. Upon review, the ISO identifies a new requirement to implement

two-factor authentication on the company's wireless system. Due to budget constraints, the company will be unable to implement the requirement for the next two years. The ISO is required to submit a policy exception form to the Chief Information Officer (CIO). Which of the following are MOST important to include when submitting the exception form? (Select THREE).

A. Business or technical justification for not implementing the requirements.

B. Risks associated with the inability to implement the requirements.

C. Industry best practices with respect to the technical implementation of the current controls.

D. All sections of the policy that may justify non-implementation of the requirements.

E. A revised DRP and COOP plan to the exception form.

F. Internal procedures that may justify a budget submission to implement the new requirement.

G. Current and planned controls to mitigate the risks.

Answer: A, B, G