



CAS-003^{Q&As}

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/cas-003.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





QUESTION 1

A Chief Information Security Officer (CISO) has launched an initiative to create a robust BCP/DR plan for the entire company. As part of the initiative, the security team must gather data supporting operational importance for the applications

used by the business and determine the order in which the applications must be brought back online.

Which of the following should be the FIRST step taken by the team?

- A. Perform a review of all policies and procedures related to BCP and DR and create an educational module that can be assigned to all employees to provide training on BCP/DR events.
- B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
- C. Have each business unit conduct a BIA and categorize the applications according to the cumulative data gathered.
- D. Implement replication of all servers and application data to back up datacenters that are geographically dispersed from the central datacenter and release an updated BPA to all clients.

Correct Answer: C

QUESTION 2

An SQL database is no longer accessible online due to a recent security breach. An investigation reveals that unauthorized access to the database was possible due to an SQL injection vulnerability. To prevent this type of breach in the future, which of the following security controls should be put in place before bringing the database back online? (Choose two.)

- A. Secure storage policies
- B. Browser security updates
- C. Input validation
- D. Web application firewall
- E. Secure coding standards
- F. Database activity monitoring
- G.

Correct Answer: CF

QUESTION 3

To meet a SLA, which of the following documents should be drafted, defining the company's internal interdependent



unit responsibilities and delivery timelines.

- A. BPA
- B. OLA
- C. MSA
- D. MOU

Correct Answer: B

OLA is an agreement between the internal support groups of an institution that supports SLA. According to the Operational Level Agreement, each internal support group has certain responsibilities to the other group. The OLA clearly depicts the performance and relationship of the internal service groups. The main objective of OLA is to ensure that all the support groups provide the intended ServiceLevelAgreement.

QUESTION 4

A company is in the process of implementing a new front end user interface for its customers, the goal is to provide them with more self-service functionality. The application has been written by developers over the last six months and the project is currently in the test phase.

Which of the following security activities should be implemented as part of the SDL in order to provide the MOST security coverage over the solution? (Select TWO).

- A. Perform unit testing of the binary code
- B. Perform code review over a sampling of the front end source code
- C. Perform black box penetration testing over the solution
- D. Perform grey box penetration testing over the solution
- E. Perform static code review over the front end source code

Correct Answer: DE

With grey box penetration testing it means that you have limited insight into the device which would most probable by some code knowledge and this type of testing over the solution would provide the most security coverage under the circumstances.

A Code review refers to the examination of an application (the new network based software product in this case) that is designed to identify and assess threats to the organization. With a static code review it is assumed that you have all the sources available for the application that is being examined. By performing a static code review over the front end source code you can provide adequate security coverage over the solution.

QUESTION 5

A company's existing forward proxies support software-based TLS decryption, but are currently at 60% load just dealing with AV scanning and content analysis for HTTP traffic. More than 70% outbound web traffic is currently encrypted. The switching and routing network infrastructure precludes adding capacity, preventing the installation of a dedicated TLS decryption system. The network firewall infrastructure is currently at 30% load and has software



decryption modules that can be activated by purchasing additional license keys. An existing project is rolling out agent updates to end-user desktops as part of an endpoint security refresh.

Which of the following is the BEST way to address these issues and mitigate risks to the organization?

- A. Purchase the SSL, decryption license for the firewalls and route traffic back to the proxies for end-user categorization and malware analysis.
- B. Roll out application whitelisting to end-user desktops and decommission the existing proxies, freeing up network ports.
- C. Use an EDP solution to address the malware issue and accept the diminishing role of the proxy for URL categorization in the short term.
- D. Accept the current risk and seek possible funding approval in the next budget cycle to replace the existing proxies with ones with more capacity.

Correct Answer: B

[CAS-003 PDF Dumps](#)

[CAS-003 VCE Dumps](#)

[CAS-003 Exam Questions](#)