CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

https://www.leads4pass.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties.

Which of the following should be implemented to BEST manage the risk?

A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewals. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit clause. Regularly assess the supplier\\'s post-contract renewal with a dedicated risk management team.

B. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all suppliers. Store findings from the reviews in a database for all other business units and risk teams to reference.

C. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.

D. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed and managed based on the supplier\\'s rating. Report finding units that rely on the suppliers and the various risk teams.

Correct Answer: A

QUESTION 2

When managing and mitigating SaaS cloud vendor risk, which of the following responsibilities belongs to the client?

A. Data

B. Storage

C. Physical security

D. Network

Correct Answer: A

QUESTION 3

A security analyst is performing a review of a web application. During testing as a standard user, the following error log appears:

```
Error Message in Database Connection
Connection to host USA-WebApp-Database failed
Database "Prod-DB01" not found
Table "CustomerInfo" not found
Please retry your request later
```

Which of the following BEST describes the analyst\\'s findings and a potential mitigation technique?

A. The findings indicate unsecure references. All potential user input needs to be properly sanitized.

B. The findings indicate unsecure protocols All cookies should be marked as HttpOnly.

C. The findings indicate information disclosure. The displayed error message should be modified.

D. The findings indicate a SQL injection. The database needs to be upgraded.

Correct Answer: C

QUESTION 4

A penetration tester is trying to gain access to a building after hours as part of a physical assessment of an office complex. The tester notes that each employee touches a badge near a small black box outside the side door, and the door unlocks. The tester uses a software-defined radio tool to determine a 125kHz signal is used during this process. Which of the following technical solutions would be BEST to help the penetration tester gain access to the building?

A. Generate a 125kHz tone.

B. Compromise the ICS/SCADA system.

C. Utilize an RFID duplicator.

D. Obtain a lock pick set.

Correct Answer: A

QUESTION 5

An analyst received a list of IOCs from a government agency. The attack has the following characteristics:

1.

The attack starts with bulk phishing.

2.

If a user clicks on the link, a dropper is downloaded to the computer.

3.

Each of the malware samples has unique hashes tied to the user.

The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

A. Update the incident response plan.

B. Blocklist the executable.

C. Deploy a honeypot onto the laptops.

D. Detonate in a sandbox.

Correct Answer: D