



GCCC^{Q&As}

GCCC - GIAC Critical Controls Certification (GCCC)

Pass GIAC GCCC Exam with 100% Guarantee

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

<https://www.pass4itsure.com/gcccc.html>

100% Passing Guarantee
100% Money Back Assurance

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

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



**QUESTION 1**

An auditor is validating the policies and procedures for an organization with respect to a control for Data Recovery. The organization's control states they will completely back up critical servers weekly, with incremental backups every four hours. Which action will best verify success of the policy?

- A. Verify that the backup media cannot be read without the encryption key
- B. Check the backup logs from the critical servers and verify there are no errors
- C. Select a random file from a critical server and verify it is present in a backup set
- D. Restore the critical server data from backup and see if data is missing

Correct Answer: D

QUESTION 2

An organization is implementing an application software security control their custom-written code that provides web-based database access to sales partners. Which action will help mitigate the risk of the application being compromised?

- A. Providing the source code for their web application to existing sales partners
- B. Identifying high-risk assets that are on the same network as the web application server
- C. Creating signatures for their IDS to detect attacks specific to their web application
- D. Logging the connection requests to the web application server from outside hosts

Correct Answer: C

QUESTION 3

A breach was discovered after several customers reported fraudulent charges on their accounts. The attacker had exported customer logins and cracked passwords that were hashed but not salted. Customers were made to reset their passwords.

Shortly after the systems were cleaned and restored to service, it was discovered that a compromised system administrator's account was being used to give the attacker continued access to the network. Which CIS Control failed in the continued access to the network?

- A. Maintenance, Monitoring, and Analysis of Audit Logs
- B. Controlled Use of Administrative Privilege
- C. Incident Response and Management
- D. Account Monitoring and Control

Correct Answer: C



QUESTION 4

Which of the following statements is appropriate in an incident response report?

- A. There had been a storm on September 27th that may have caused a power surge
- B. The registry entry was modified on September 29th at 22:37
- C. The attacker may have been able to access the systems due to missing KB2965111
- D. The backup process may have failed at 2345 due to lack of available bandwidth

Correct Answer: B

QUESTION 5

What could a security team use the command line tool Nmap for when implementing the Inventory and Control of Hardware Assets Control?

- A. Control which devices can connect to the network
- B. Passively identify new devices
- C. Inventory offline databases
- D. Actively identify new servers

Correct Answer: D

[GCCC PDF Dumps](#)

[GCCC Study Guide](#)

[GCCC Braindumps](#)