GAQM®
Global Association for Quality Management

Exam Name – Certified Information Systems Security Tester (CISST)™

Exam Code – CISST-001

Sample Exam

(Question): Which of the following is a purpose of a security audit?

(A): To prevent users from using simple passwords
(B): To reveal insufficient patch updates provided by the vendor
(C): To halt unauthorized intruders from accessing the system
(D): To require users to change their password after a predetermined set of days

(Correct): B

(Question): You are responsible for ensuring that new vendors brought on externally for the project are fully compliant with government mandated guidelines as part of your risk assessment. On which stakeholders should you primarily focus to ensure these outside vendors continue to comply?

(A): Customers, users, and vendors to ensure there is good communication between them
(B): Public users and vendors who will follow the law as it applies to the source of information
(C): Federal and local agencies that communicate guidelines to follow
(D): Both internal and external sources that will use the information for further analyzing the risk

(Correct): C

(Question): Which of the following is a consequence of a policy that minimizes access to a system or device to acceptable levels?

(A): More devices are added to mitigate the impact
(B): Proper controls of self-provisioning devices such as routers are prohibited
(C): Devices that do not conform are removed from the wireless network
(D): Access to the VPN is severely restricted

(Correct): C

(Question): Your role as the Security Administrator is to help your organization understand the effectiveness of security policies and procedures across the enterprise. You will report your effectiveness findings to Senior Management after your analysis has been completed. Which of the following is the optimum strategy to accomplish this?

(A): Implement a static analysis evaluation independently for both policies and procedures
(B): Analyze the results from a security test to validate effectiveness
(C): Evaluate security test results that focus on current threats and attacks
(D): Evaluate the static test results for new and emerging software threats

(Correct): B

(Question): If an organization experiences a security breach and legal action results, how does it help the organization to have done security testing?

(A): It can show that the organization has done due diligence to try to prevent such an incident
(B): The documentation from the security testing can be used to track down the perpetrator
(C): Since any important information would have been backed up before security testing, this backup can be used to restore any compromised information
(D): By tracing through the documented tests, the security testing team can discover how the breach was possible

(Correct): A

(Question): You are working at a bank as part of the security testing team. During a recent security audit it was noted that the user's passwords were not strong enough. Since that time, a new set of requirements has been issued to ensure password strength. Given this information, what would be a reasonable set of security objectives for general password rule testing?

1. Verify that passwords meet the requirements for length

2. Verify that passwords meet the requirements for usage of characters, numbers, letters and capitalization

3. Verify that passwords can be retried three times

4. Verify that passwords cannot be re-used within a one year timeframe

5. Verify that passwords must be reset every three months

6. Verify that the user can request to have their password emailed to them

(Question): Verify that the system administrator can reset a locked password

(A): 1, 2, 3, 4
(B): 1, 2, 4, 5
(C): 3, 4, 6, 7
(D): 4, 5, 6, 7

(Correct): B

(Question): Which of the following would be revealed during an audit of security practices?

(A): Misconfiguration of a firewall zone
(B): Inadequate application of security updates from a software vendor
(C): Levels of risk for digital and physical assets
(D): Stakeholder responsibilities in information security practices

(Correct): B