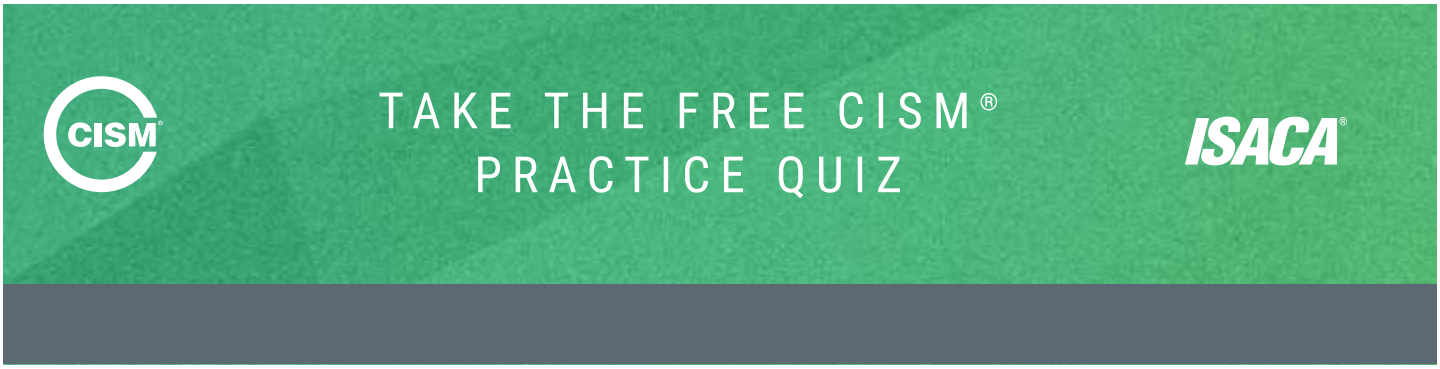

YOU DIDN'T PASS WITH 4/10 CORRECT, BUT YOU CAN STILL EXCEL ON THE EXAM!

Great effort! No matter your score, the right preparation from ISACA® will help you excel on your CISM® exam and move your career forward.

Scroll down for your detailed results.

Remember: these questions are a small preview of what you can expect on exam day. The official CISM exam has 150 questions.

You're just a few steps away from obtaining your CISM certification:

1. Prep for your exam.
2. Register and pay for your exam.
3. Schedule your exam.
4. Ace the CISM exam.

Choose the Exam Prep that Best Fits Your Needs.

EXPLORE CISM PREP

Master the CISM material

Quickly expand your skillset

Become better at your job

Make the most of exam day

TRAINED BY ISACA®. CERTIFIED BY ISACA.

1

A risk assessment and business impact analysis (BIA) have been completed for a major proposed purchase and new process for an organization. There is disagreement between the information security manager and the business department manager who will be responsible for evaluating the results and

identified risk. Which of the following would be the **BEST** approach of the information security manager?

YOUR ANSWER: D. Create a new risk assessment and BIA to resolve the disagreement

CORRECT ANSWER: C. Review of the risk assessment with executive management for final input

EXPLANATION: There is no indication that the assessments are inadequate or defective in some way; therefore, repeating the exercise is not warranted.

2 ✗

Who is accountable for ensuring that information is categorized and that specific protective measures are taken?

YOUR ANSWER: D. The custodian

CORRECT ANSWER: B. Senior management

EXPLANATION: The custodian supports and implements information security measures as directed.

3 ✓

Abnormal server communication from inside the organization to external parties may be monitored to:

YOUR ANSWER: A. record the trace of advanced persistent threats

EXPLANATION: The most important feature of target attacks as seen in advanced persistent threats is that malware secretly sends information back to a command and control server. Therefore, monitoring of outbound server communications that do not follow predefined routes will be the best control to detect such security events.

4 ✓

Which of the following authentication methods prevents authentication replay?

YOUR ANSWER: B. Challenge/response mechanism

EXPLANATION: A challenge/response mechanism prevents replay attacks by sending a different random challenge in each authentication event. The response is linked to that challenge.

5

IT-related risk management activities are **MOST** effective when they are:

YOUR ANSWER: D. communicated to all employees

CORRECT ANSWER: C. integrated within business processes

EXPLANATION: Communication alone does not necessarily correlate with successful execution of the process.

6

Which of the following is the **BEST** way to detect an intruder who successfully penetrates a network before significant damage is inflicted?

YOUR ANSWER: A. Perform periodic penetration testing

CORRECT ANSWER: D. Install a honeypot on the network

EXPLANATION: Penetration testing will not detect an intruder.

7

Which of the following presents the **GREATEST** threat to the security of an enterprise resource planning (ERP) system?

YOUR ANSWER: D. Database security defaults to ERP settings

CORRECT ANSWER: C. Operating system security patches have not been applied

EXPLANATION: Database security defaulting to the enterprise resource planning system's settings is not as significant.

8

In a social engineering scenario, which of the following will **MOST** likely reduce the likelihood of an unauthorized individual gaining access to computing resources?

YOUR ANSWER: B. Conducting periodic security awareness programs

EXPLANATION: Social engineering can best be mitigated through periodic security awareness training for users who may be the target of such an attempt.

9

The postincident review of a security incident revealed that there was a process that was not monitored. As a result monitoring functionality has been

implemented. Which of the following may **BEST** be expected from this remediation?

YOUR ANSWER: B. Increase in risk tolerance

CORRECT ANSWER: C. Improvement in identification

EXPLANATION: Risk tolerance is a determination made by senior management based on the results of a risk analysis and the amount of risk senior management believes the organization can manage effectively. Risk tolerance will not change from implementation of a monitoring process.

10 ✓

To determine how a security breach occurred on the corporate network, a security manager looks at the logs of various devices. Which of the following **BEST** facilitates the correlation and review of these logs?

YOUR ANSWER: C. Time server

EXPLANATION: To accurately reconstruct the course of events, a time reference is needed, and that is provided by the time server.