

Exam Name - Certified Information Security Officer (CISO)™

Sample Exam

- 1.** What is the MAIN purpose of a Security Operations Center (SOC)?
- A. Provide Tier 1 technical support
 - B. Consolidate security event logs
 - C. Coordinate people, processes, and tech to detect and respond to incidents
 - D. Assist governments with cybercrime intelligence

Answer **C**

- 2.** As CISO, with a range of audit findings (High/Med/Low), which is the BEST action?
- A. Remediate high-impact compliance issues first
 - B. Focus only on non-compliant findings
 - C. Fix low issues to boost audit visibility
 - D. Remediate medium issues unless under compliance scope

Answer **A**

- 3.** If a critical vulnerability blocks release, what should be evaluated to reduce risk?
- A. Developer security training
 - B. Compensating Controls
 - C. Deploy IDS
 - D. New security tools

Answer **B**

4. What factor is MOST important to a CISO's success?

- A. Audit scores
- B. Consultant recommendations
- C. Senior leadership relationships
- D. Employee security awareness

Answer **C**

5. Define the "critical path" in project management terms.

- A. Tasks that, if delayed, affect project end-date
- B. Tasks not critical to project
- C. Tasks too costly to delay
- D. Tasks that pivot project direction

Answer **A**

6. Which network control best prevents unauthorized data removal by employees?

- A. DLP solution
- B. Syslog reviews
- C. Deploy IDS
- D. Security guards

Answer **A**