



Sample Exam

Exam Name: Certified Incident Manager (CIM)

Exam Code: CIM-001

1. Which factor MOST directly differentiates incident prioritization from incident classification?

- A. Incident classification determines response ownership
- B. Incident prioritization evaluates urgency and business impact
- C. Classification focuses on lifecycle phases
- D. Prioritization defines root cause analysis

Correct Answer: B

2. Which phase of the incident lifecycle primarily ensures that lessons learned contribute to organizational resilience?

- A. Detection
- B. Response
- C. Closure
- D. Recovery

Correct Answer: C

3. According to the historical evolution of incident management, what major development shifted incident management from reactive to structured practices?

- A. Rise of cybersecurity threats
- B. Development of personal computers
- C. Introduction of ITIL framework
- D. Expansion of cloud computing

Correct Answer: C

4. In incident management frameworks, why is role delineation considered critical during high-severity incidents?

- A. It improves incident detection accuracy
- B. It prevents regulatory non-compliance
- C. It reduces confusion and duplication of effort
- D. It ensures faster post-incident reporting

Correct Answer: C

5. Which activity BEST characterizes the mitigation phase during response and containment?

- A. Isolating affected systems
- B. Blocking malicious traffic
- C. Applying patches and restoring backups
- D. Logging incident details

Correct Answer: C

6. Why is dynamic reassessment essential during assessment and prioritization?

- A. Incident severity always increases
- B. Business priorities may shift
- C. Monitoring tools may fail
- D. Stakeholders demand constant updates

Correct Answer: B

7. Which outcome MOST directly results from ineffective detection and reporting mechanisms?

- A. Increased regulatory penalties
- B. Delayed incident containment
- C. Poor post-incident documentation
- D. Weak governance frameworks

Correct Answer: B
