CompTIA CS0-004 Dumps

Shared by Schwartz on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A vulnerability analyst runs a credentialed vulnerability scan covering all addressable enterprise assets. After running the scan, the analyst discovers a large number of critical vulnerabilities that cannot be immediately remediated.

Which of the following are the most likely reasons why the vulnerabilities cannot be immediately addressed?

Options:

A- Lack of technical skills, the absence of a test environment, and the absence of an asset inventory
B- Physical access challenges, the absence of vendor support, and a lack of system documentation
C- Inaccurate asset inventory, a lack of system documentation, and an absence of authorization
D- Legacy and proprietary systems, a lack of patch availability, and vendor dependencies

Answer:

D

Explanation:

Legacy and proprietary systems, unavailable patches, and vendor dependencies are classic technical and operational inhibitors to immediate vulnerability remediation. A legacy application may require obsolete libraries or operating systems that cannot accept modern updates. Proprietary platforms may permit changes only through an approved manufacturer or integrator, while certain vulnerabilities simply have no patch available when they are initially disclosed.

CISA guidance emphasizes continuously monitoring vendor vulnerability and patch announcements because remediation frequently depends on vendor-provided updates. CISA and NIST guidance also recognizes that systems remaining in service after vendor support ends create significant vulnerability-management challenges because patches may no longer be produced.

Option A is weakened by ''absence of an asset inventory'' because the scenario states that the credentialed scan already covers all addressable enterprise assets; inventory quality can affect management, but it does not best explain why identified critical findings cannot be patched. Options B and C contain possible administrative difficulties, yet they are less directly tied to widespread remediation constraints.

When immediate remediation is impossible, analysts should document the exception, assess risk, apply compensating controls where feasible, monitor affected systems, and establish a migration or vendor-remediation plan.

Study Guide Reference: Vulnerability Management Remediation Constraints Legacy/Proprietary Systems Patch Availability Vendor Dependencies Compensating Controls Risk Acceptance/Exception Management.

Question 2

Question Type: MultipleChoice

A security operations center (SOC) manager reviews a document signed by the Chief Financial Officer (CFO), the sales director, and a customer to decide whether a contract breach occurred.

Which of the following best describes the document that includes key performance indicators (KPIs)?

Options:

A- Tactics, techniques, and procedures (TTPs)
B- Return on investment report
C- Service-level agreement (SLA)
D- Risk management plan
E- Memorandum of understanding

Answer:

C

Explanation:

A service-level agreement (SLA) formally establishes measurable service expectations between a provider and a customer. These expectations commonly include availability targets, response times, resolution times, service quality thresholds, escalation conditions, reporting requirements, and other measurable performance indicators. NIST describes an SLA as a document that specifies technical performance promises and how performance or disputes will be handled. NIST security-control guidance also notes that service-level agreements can define performance expectations and measurable outcomes.

That makes an SLA the appropriate document when management needs to determine whether contractual performance requirements were violated. KPIs contained in the agreement provide

objective measures against which actual service performance can be compared.

TTPs describe adversary behavior and have no contractual purpose. A return-on-investment report evaluates financial effectiveness rather than service obligations. A risk management plan describes how organizational risks will be identified and treated. A memorandum of understanding records cooperation or intent between parties, but it typically does not provide the detailed operational performance guarantees associated with an SLA.

The clues are customer, signed agreement, contractual breach, and measurable KPIs---all of which strongly identify a service-level agreement.

Study Guide Reference: Reporting and Communication Service-Level Agreements KPIs Contractual Requirements Performance Metrics Compliance and Escalation.

Question 3

Question Type: MultipleChoice

Which of the following contains stakeholder contact information for incident response reporting?

Options:

A- The company organization chart
B- The communication plan
C- The last incident report
D- The standard operating procedures

Answer:

B

Explanation:

The communication plan is the appropriate document because it establishes who must be contacted during an incident, how communications should occur, which channels are authorized, and how information should be escalated to internal and external stakeholders.

Incident-response communications may involve security personnel, executive leadership, legal counsel, privacy teams, public relations, human resources, business owners, vendors, regulators, law enforcement, customers, and other parties depending on incident severity. NIST's incident-response guidance emphasizes coordination with relevant stakeholders as part of an effective response capability. A communication plan operationalizes that requirement by maintaining

contact information, responsibilities, escalation paths, notification requirements, and approved communication methods.

An organization chart identifies reporting relationships but may not contain emergency contact details, alternate channels, external contacts, or escalation procedures. A previous incident report documents a historical event and should not be treated as the authoritative contact source. Standard operating procedures can describe technical or administrative steps, but stakeholder communications are more appropriately centralized in the incident communication plan.

Maintaining this information in advance is critical because incident response frequently occurs under time pressure and may involve unavailable or compromised normal communication systems.

Study Guide Reference: Reporting and Communication Communication Plan Stakeholder Contacts Escalation Paths Internal/External Notifications Out-of-Band Communications.

Question 4

Question Type: MultipleChoice

Which of the following does a phishing campaign click rate measure?

Options:

A- The effectiveness of an organization's email filters
B- The false-positive rate of data leakage prevention behavior
C- The employees' security awareness
D- The speed of responding to a social engineering attack

Answer:

C

Explanation:

A phishing simulation click rate measures user susceptibility to phishing and is therefore primarily an indicator of employee security awareness and behavior. If a simulated phishing message is delivered to employees and a percentage of recipients click the embedded malicious-style link, that percentage provides evidence about how effectively users are recognizing and resisting social-engineering attempts.

NIST research specifically identifies phishing-simulation click rates as a commonly used measure for evaluating the effectiveness of phishing-related security-awareness programs. NIST also cautions that raw click rates should be interpreted in context because phishing messages differ substantially in difficulty; the Phish Scale was developed to provide context for click-rate and report-rate results.

The metric does not primarily measure email-filter effectiveness because a controlled simulation may intentionally bypass or be allowlisted through technical filtering so employee behavior can be evaluated. It is unrelated to data-loss prevention false positives. It also does not directly measure response speed; metrics such as reporting time or mean time to respond would be more appropriate for that purpose.

Therefore, click rate is fundamentally a human-risk and awareness metric.

Study Guide Reference: Reporting and Communication Security Metrics Security Awareness Phishing Simulations Click Rate Reporting Rate Human Risk Measurement.

Question 5

Question Type: MultipleChoice

Which of the following will inhibit remediation when attempting to resolve a vulnerability?

Options:

A- Controlled systems
B- Legacy systems
C- Shared systems
D- Closed systems

Answer:

B

Explanation:

Legacy systems commonly inhibit vulnerability remediation because they may depend on obsolete operating systems, unsupported applications, specialized hardware, outdated protocols, or vendor products for which security updates are no longer provided. Even when a vulnerability is accurately identified, the organization may be unable to apply a modern patch without breaking compatibility, interrupting a critical business process, or violating vendor support requirements.

NIST guidance explicitly recognizes that legacy systems create unique security-management challenges, while federal cybersecurity guidance warns that products remaining in service after vendor support ends may lack effective mechanisms for addressing newly discovered vulnerabilities.

In such circumstances, vulnerability-management teams may need to use compensating controls such as segmentation, firewall restrictions, application allowlisting, stronger access controls, enhanced monitoring, or service isolation while planning migration or replacement. These controls reduce exposure but do not remove the underlying software defect.

''Controlled systems,'' ''shared systems,'' and ''closed systems'' do not inherently prevent remediation. A shared system may require greater coordination, but it can still be fully supported and patchable. The defining issue with legacy technology is that technical and vendor constraints can directly prevent normal remediation.

Study Guide Reference: Vulnerability Management Remediation Constraints Legacy Systems End-of-Life Technology Patch Availability Compensating Controls System Replacement.

Question 6

Question Type: MultipleChoice

A Chief Information Security Officer (CISO) is notified of an ongoing incident.

Which of the following explains why the CISO instructs the Chief Executive Officer not to discuss the incident over email?

Options:

A- The security team discovered a vulnerability in the Short Message Service email gateway.
B- The email system may be compromised.
C- Emails are not encrypted in transit.
D- The CISO has not notified the public relations team of the incident.

Answer:

B

Explanation:

During an active cybersecurity incident, responders must assume that systems associated with the compromise may no longer provide trustworthy confidentiality or integrity until their status

has been established. If the incident could involve the organization's email infrastructure, discussing response strategy, investigative findings, affected assets, or containment actions through corporate email could unintentionally provide the attacker with intelligence about the organization's response.

Therefore, the email system may be compromised is the strongest explanation. Incident-response communication plans should define approved communication methods, relevant stakeholders, escalation paths, and alternative communication channels so responders can continue coordinating when ordinary enterprise systems are unavailable or untrusted. NIST's current incident-response guidance emphasizes integrating communication and stakeholder coordination throughout response activities.

Option C is too broad. Modern email commonly uses transport encryption, although encryption alone would not make a compromised mailbox or server trustworthy. Option D concerns public-relations coordination but does not explain why email itself should be avoided. Option A describes a specific gateway vulnerability that the scenario does not establish.

The core principle is out-of-band communication: when normal communication infrastructure may be under attacker control, responders should use a previously approved independent channel.

Study Guide Reference: Reporting and Communication Incident Communications Communication Plan Out-of-Band Communications Stakeholder Coordination Compromised Communication Channels.

Question 7

Question Type: MultipleChoice

Which of the following is the most comprehensive type of report associated with a closed incident?

Options:

A- Lessons-learned
B- Situation
C- Root cause analysis
D- After action

Answer:

D

Explanation:

An after-action report (AAR) is the most comprehensive document associated with a closed incident because it consolidates the incident itself, the response activities performed, recovery actions, outcomes, deficiencies, and lessons identified during the event. NIST Cybersecurity Framework guidance specifically calls for preparing an after-action report that documents the incident, response and recovery activities, and lessons learned.

A lessons-learned document focuses primarily on what worked, what failed, and what should be improved. Those observations are important, but they represent only one component of a complete post-incident record. Root cause analysis has a narrower technical purpose: determining the fundamental condition that permitted the incident to occur or progress. A situation report is generally produced while an incident is ongoing to communicate current status, impact, actions, and outstanding issues.

An AAR is broader because it can incorporate the timeline, technical findings, containment and eradication actions, recovery results, stakeholder performance, root cause, lessons learned, and assigned corrective actions. NIST exercise guidance likewise treats lessons learned as information that becomes part of an after-action report.

Study Guide Reference: Reporting and Communication Post-Incident Reporting After-Action Reports Lessons Learned Root Cause Analysis Corrective Actions.

Question 8

Question Type: MultipleChoice

A security operations center manager is concerned that after action reporting is not being completed in a timely manner.

Which of the following will allow the manager to quantify this concern?

Options:

A- Mean time to remediate
B- Mean time to close
C- Mean time between failures
D- Mean time to respond

Answer:

B

Explanation:

Mean time to close is the most relevant measurement because the manager needs to quantify how long cases or incidents remain open before all required closure activities---including after-action documentation---are completed.

An incident may already be technically contained and remediated while administrative closure remains outstanding. Mean time to remediate measures how long it takes to correct or neutralize the security problem, but it does not necessarily include final reporting and formal case closure. Mean time to respond measures how quickly responders begin or perform response activity after detection. Mean time between failures is primarily a reliability metric describing the average operating duration between failures and does not measure SOC reporting performance.

Current Microsoft Sentinel SOC guidance explicitly includes mean time to closure and time-to-closure percentiles among incident-management metrics used to evaluate SOC performance. This directly maps to the manager's concern: if after-action reports delay completion of incidents, the organization's mean closure time will increase and can be trended by analyst, severity, team, or incident category.

Therefore, B provides the quantitative evidence needed to determine whether after-action reporting is preventing incidents from being closed promptly.

Study Guide Reference: Reporting and Communication Incident Metrics Mean Time to Close After-Action Reporting SOC Performance Measurement Continuous Improvement.

Question 9

Question Type: MultipleChoice

Which of the following is commonly used after an incident has been resolved to identify efficiencies and corrective actions related to activities performed during the incident response process?

Options:

A- Lessons learned
B- Key performance indicators (KPIs) and performance metrics
C- Executive summary
D- Root cause analysis

Answer:

A

Explanation:

A lessons learned review evaluates how the incident was handled and identifies improvements that should be incorporated into future response activities. It examines what worked well, what created delays, where communications or escalation failed, whether tools and playbooks were effective, and which corrective actions should be assigned to reduce the likelihood or impact of similar incidents.

NIST's current incident-response guidance places strong emphasis on continuous improvement. It states that lessons identified during incident-response activities should feed into organizational improvement so policies, processes, practices, and security capabilities can be adjusted as necessary. NIST also notes that traditional post-incident activities identify required improvements and return them to preparation and broader cybersecurity risk management.

KPIs quantify operational performance but do not themselves provide the qualitative review necessary to identify process efficiencies and corrective actions. An executive summary communicates major incident facts and outcomes to leadership. Root cause analysis focuses on identifying the fundamental technical or organizational cause of the incident; it can contribute to lessons learned but is narrower in scope.

Therefore, the broader mechanism for reviewing the entire response process and developing improvement actions is the lessons-learned process.

Study Guide Reference: Reporting and Communication Post-Incident Reporting Lessons Learned Corrective Actions Process Improvement Stakeholder Feedback.