ISACA CISM Exam Questions

Total Questions: 930+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: CISM Exam Dumps by Cert Empire

Question: 1

The MAIN benefit of implementing a data loss prevention (DLP) solution is to:

A: enhance the organization's antivirus controls.

B: eliminate the risk of data loss.

C: complement the organization's detective controls.

D: reduce the need for a security awareness program.

Correct Answer:

C

Explanation:

The main benefit of a Data Loss Prevention (DLP) solution is to complement an organization's existing control framework, specifically its detective controls. DLP systems operate by inspecting data in use, in motion, or at rest to detect sensitive information that violates a predefined policy. This content-aware detection capability fills a critical gap left by traditional security tools like firewalls or intrusion detection systems (IDS), which typically lack deep visibility into data content. By adding this specific, data-centric detective layer, DLP enhances the organization's ability to identify potential data breaches, which is the necessary first step to preventing them.

Why Incorrect Options are Wrong:

A: Antivirus is designed to combat malware, whereas DLP is designed to protect data content. They are different, though complementary, security technologies.

B: No single control can "eliminate" risk. According to risk management principles, DLP is a control that mitigates or reduces the risk of data loss, but it cannot completely eliminate it.

D: DLP is a technical control that often works in concert with administrative controls like security awareness programs; it does not reduce the need for them.

References:

1. ISACA CISM Review Manual, 15th Edition: While not providing a direct quote for this specific question, the manual's discussion of security controls in Domain 3, "Information Security Program Development and Management," positions DLP as a technology that enforces data handling policies. Its function is to detect potential violations and prevent data leakage, thereby acting as both a detective and preventive control that complements the overall security architecture.

2. Stanford University - University IT: "Data Loss Prevention (DLP) is a strategy and a set of tools to ensure that sensitive data is not lost, misused, or accessed by unauthorized users... DLP software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to detect and prevent the unauthorized use and transmission of sensitive data." This description highlights the dual detect-and-prevent function, where detection is a foundational component that complements other network monitoring. (URL: https://uit.stanford.edu/guide/dlp)

3. Purdue University - Secure Purdue: "Data Loss Prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations..." This emphasizes the classification and identification (detection) process as core to its function, which complements other controls. (URL: https://www.purdue.edu/securepurdue/data-handling/data-loss-prevention.php)

Question: 2

During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?

A: Post-incident review

B: Eradication

C: Containment

D: Identification

Correct Answer:

B

Explanation:

The Eradication phase is dedicated to the removal of the incident's root cause and all its components from the affected systems. According to the NIST incident response lifecycle, this phase involves actions such as deleting malware, disabling breached accounts, and identifying and mitigating the exploited vulnerabilities. To ensure a thorough and effective removal, the incident response team must first identify and document the specific actions required to eliminate the threat completely. This documentation guides the systematic execution of the eradication process and helps prevent re-infection.

Why Incorrect Options are Wrong:

A: Post-incident review: This phase analyzes the completed incident response effort for lessons learned; it does not involve planning the active removal of a threat.

C: Containment: This phase focuses on limiting the spread and impact of an ongoing incident, not on the permanent removal of the threat's cause.

D: Identification: This phase involves detecting and validating that an incident has occurred, which happens before any remediation or removal actions are planned.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-61 Rev. 2, "Computer Security Incident Handling Guide": Section 3.3.3, "Containment, Eradication, and Recovery," states that in the eradication phase, the team "eliminates components of the incident, such as deleting malware and disabling breached user accounts." This inherently includes the planning and documentation of those removal actions. (URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, Page 26)

2. ISACA, "Responding to Targeted Cyberattacks" White Paper: This document outlines the incident response process, aligning with the NIST model. It describes eradication as the phase where the "cause of the compromise is removed," which necessitates planning and documenting the removal steps. (Available through ISACA official resources for members).

3. Carnegie Mellon University, Software Engineering Institute, "Defining Incident Management Processes": Courseware and publications from CERT/CC (a division of SEI) consistently define eradication as the phase for eliminating the cause of the incident, a step that requires careful planning and documentation of actions. (Reference: General principles outlined in CERT materials on incident management).

Question: 3

Which of the following is PRIMARILY determined by asset classification?

A: Insurance coverage required for assets

B: Level of protection required for assets

C: Priority for asset replacement

D: Replacement cost of assets

Correct Answer:

B

Explanation:

The primary purpose of asset classification is to categorize information and other assets based on their level of value, sensitivity, and criticality to the organization. This classification directly determines the appropriate level of security controls and protection that must be implemented to safeguard the asset. For example, an asset classified as "Restricted" will require more stringent access controls, encryption, and handling procedures than one classified as "Public." This ensures that security resources are applied in a cost-effective manner, commensurate with the asset's importance.

Why Incorrect Options are Wrong:

A: Insurance coverage required for assets: Insurance is a form of risk treatment. While asset value (part of classification) informs this decision, it is a secondary consideration, not the primary driver for classification.

C: Priority for asset replacement: This is a key consideration for business continuity and disaster recovery planning, but the primary purpose of classification is to define ongoing, day-to-day protection levels.

D: Replacement cost of assets: Replacement cost is an input to the asset valuation process, which is a component of classification. The classification itself does not determine the cost; rather, the cost helps determine the classification.

References:

1. ISACA CISM Review Manual, 16th Edition. Domain 2: Information Risk Management, Section 2.4 Information Asset Classification. The manual explicitly states, "The primary purpose of information classification is to ensure that information assets receive an

appropriate level of protection." It further details that classification schemes are the basis for applying security controls.

2. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. This academic article discusses the foundations of information security, noting that classification is a fundamental step to "apply appropriate security controls" based on the information's value and sensitivity. (Available via academic databases like IEEE Xplore or ScienceDirect).

3. Peltier, T. R. (2013). Information Security Risk Analysis, Third Edition. CRC Press (Taylor & Francis Group). Chapter 5, "Risk Assessment," details that asset classification is performed to "determine the level of protection needed for the organization’s information assets." This establishes a direct link between classification and protection levels.

Question: 4

ACISO learns that a third-party service provider did not notify the organization of a data breach that affected the service provider's data center. Which of the following should the CISO do FIRST?

A: Recommend canceling the outsourcing contract.

B: Request an independent review of the provider's data center.

C: Notify affected customers of the data breach.

D: Determine the extent of the impact to the organization.

Correct Answer:

D

Explanation:

Upon learning of a potential incident, the immediate priority is to initiate the organization's incident response plan. The first phase of any standard response framework is identification and analysis, which involves assessing the situation to understand its scope and potential impact. This determination is a prerequisite for all other actions. It informs the containment strategy, identifies legal and contractual notification obligations, and provides the necessary context for making strategic decisions about the third-party relationship. Acting without this initial assessment is premature and can lead to ineffective or incorrect responses.

Why Incorrect Options are Wrong:

A: Recommend canceling the outsourcing contract. This is a significant business and legal decision that should only be considered after the full impact of the breach is understood.

B: Request an independent review of the provider's data center. This is a corrective or due diligence action for later, not the immediate priority of managing the current incident's impact on your organization.

C: Notify affected customers of the data breach. Notification is critical but must be based on accurate information gathered during the impact assessment to be effective and meet regulatory requirements.

References:

1. ISACA CISM Review Manual, 16th Edition. Domain 4: Information Security Incident Management. The manual details that the incident response process begins with detection,

followed immediately by analysis and assessment to determine the scope and impact, which then guides all subsequent steps like containment, eradication, and communication.

2. Everett, (2011). Third-Party Security Risk. ISACA Journal, Volume 6. This and similar articles in the ISACA Journal emphasize that when a third-party incident occurs, the organization must first invoke its own incident response plan to assess the impact on its own data and operations before taking external actions.

3. MIT OpenCourseWare. (2014). 6.857 Computer and Network Security, Fall 2014. Lecture 20: Incident Response. University courseware on incident response consistently presents a phased approach, where analysis and scoping (determining impact) are the immediate steps following detection to inform and guide the rest of the response. (Reference based on standard curriculum structure for this topic).

Question: 5

An information security manager developing an incident response plan MUST ensure it includes:

A: an inventory of critical data.

B: criteria for escalation.

C: a business impact analysis (BIA).

D: critical infrastructure diagrams.

Correct Answer:

B

Explanation:

An incident response plan (IRP) is fundamentally a procedural document that outlines the steps to be taken when an incident occurs. A critical component of this procedure is defining the criteria for escalation. Escalation procedures ensure that an incident receives the appropriate level of attention and resources based on its severity, potential impact, and complexity. This includes notifying senior management, legal counsel, or other specialized teams. Without clear escalation criteria, an organization risks mismanaging a significant incident, leading to greater damage. While other listed items are valuable, they serve as inputs or supporting artifacts rather than core procedural components within the plan itself.

Why Incorrect Options are Wrong:

A: an inventory of critical data. This is a vital input for creating the IRP and for prioritizing actions during a response, but it is a supporting document, not a core section of the plan itself.

C: a business impact analysis (BIA). The BIA is a foundational analysis that informs the IRP by identifying critical processes and impact thresholds, but it is a separate, prerequisite activity.

D: critical infrastructure diagrams. These are important supporting artifacts that are referenced by the plan to aid responders, but they are not a mandatory procedural component of the plan.

References:

1. ISACA CISM Review Manual, 16th Edition. The domain of Incident Management details that an IRP must contain clear procedures for response, including communication and escalation paths. It positions the BIA and asset inventories as inputs used to develop these procedures.

2. NIST Special Publication 800-61 Rev. 2, "Computer Security Incident Handling Guide." Section 2.3, "Incident Response Policy, Plan, and Procedure Creation," emphasizes that the plan should provide a roadmap for implementation. Section 3.1.2, "Guidelines for Communication," implicitly covers escalation by discussing who to notify and when, which must be formally defined in the plan's criteria.

3. Carnegie Mellon University, Software Engineering Institute, "Creating a Computer Security Incident Response Team." This foundational document specifies that incident response procedures must include provisions for escalation to ensure incidents are handled at the appropriate organizational level. (Reference: CMU/SEI-98-HB-001).

Question: 6

Which of the following BEST supports the incident management process for attacks on an organization's supply chain?

A: Including service level agreements (SLAs) in vendor contracts

B: Establishing communication paths with vendors

C: Requiring security awareness training for vendor staff

D: Performing integration testing with vendor systems

Correct Answer:

B

Explanation:

Effective incident management of supply-chain attacks depends on the ability to exchange alerts, indicators, and response actions with the affected supplier quickly. NIST and ISO guidance for supply-chain risk management explicitly require organizations to establish and maintain defined communication channels with suppliers so that security incidents can be reported, triaged, and remediated without delay. While SLAs and other controls may be useful, predefined communication paths are the most direct support to the incident-management process itself.

Why Incorrect Options are Wrong:

A: SLAs describe service performance; they rarely specify incident-handling contacts or procedures and therefore provide limited direct support to incident response.

C: Security awareness training is preventive, not a mechanism for coordinating or managing incidents once they occur.

D: Integration testing validates interoperability but does not address reporting or coordination when an incident in the supply chain happens.

References:

1. NIST SP 800-161r1, “Supply Chain Risk Management Practices for Systems and Organizations,” 3.2.5 Incident Response & Recovery, pp. 58-59. https://doi.org/10.6028/NIST.SP.800-161r1

2. ISO/IEC 27036-3:2013, Clause 8.4.3 “Information security incident reporting and management between organizations,” pp. 26-27. https://www.iso.org/standard/59648.html

3. NIST SP 800-171r2, Requirement 3.12.1 “Establish an incident-handling capability including external communications,” p. 77. https://doi.org/10.6028/NIST.SP.800-171r2

Question: 7

Which of the following BEST ensures information security governance is aligned with corporate governance?

A: A security steering committee including IT representation

B: A consistent risk management approach

C: An information security risk register

D: Integration of security reporting into corporate reporting

Correct Answer:

D

Explanation:

The integration of information security reporting into the standard corporate reporting cycle is the most effective mechanism for ensuring alignment. This process compels the information security function to translate technical risks and performance metrics into business-relevant terms, such as financial impact, reputational risk, and strategic objective enablement. By making security a regular agenda item for the board and senior leadership through established reporting channels, it ensures continuous oversight, accountability, and strategic alignment with overall corporate governance structures and goals.

Why Incorrect Options are Wrong:

A: A security steering committee with only IT representation is insufficient; it requires broad business leadership to ensure alignment with corporate, not just IT, objectives.

B: A consistent risk management approach is a foundational component, but it is the reporting of this risk posture to the corporate level that ensures and validates alignment.

C: An information security risk register is a tactical tool—an output of the risk management process—not the strategic mechanism that ensures governance alignment itself.

References:

1. ISACA, CISM Review Manual, 16th Edition. Chapter 1, "Information Security Governance," emphasizes that a key task is to "Establish and maintain a framework for information security governance to guide activities that support the information security strategy." A critical part of this framework is reporting to senior management and the board to provide assurance that security activities align with business objectives.

2. ISACA, COBIT 2019 Framework: Governance and Management Objectives. The governance objective EDM01 ("Ensured Governance Framework Setting and Maintenance") includes the key practice of communicating the governance framework to stakeholders. Furthermore, EDM03 ("Ensured Risk Optimisation") requires the governing body to "monitor that risk management practices are effective," which is achieved through reporting. This demonstrates that reporting is a core governance activity for ensuring alignment.

3. De Haes, S., & Van Grembergen, W. (2015). Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5. Springer International Publishing. Chapter 3 discusses governance structures, mechanisms, and processes. It highlights reporting as a key mechanism, stating, "Mechanisms such as reporting... are needed to ensure that the defined structures and processes are effectively implemented and are working." This confirms that reporting is the active mechanism for ensuring alignment.

Question: 8

Which of the following should an information security manager do FIRST upon learning that some security hardening settings may negatively impact future business activity?

A: Perform a risk assessment.

B: Reduce security hardening settings.

C: Inform business management of the risk.

D: Document a security exception.

Correct Answer:

A

Explanation:

The most appropriate initial action is to perform a risk assessment. This process formally evaluates the likelihood and impact of the negative business consequences against the security risks that the hardening settings are meant to mitigate. A risk assessment provides the objective data necessary for an informed, risk-based decision. It is the foundational step in the risk management process that must precede any decision to alter controls, formally accept risk, or escalate to management. Acting without this analysis would be premature and could lead to uninformed decisions that either expose the organization to undue risk or unnecessarily impede business operations.

Why Incorrect Options are Wrong:

B: Reduce security hardening settings: This is a potential risk treatment option, but it is inappropriate to take this action without first completing a risk assessment to understand the consequences.

C: Inform business management of the risk: While essential, this communication is most effective when supported by the data and analysis from a risk assessment, enabling management to make an informed decision.

D: Document a security exception: This is a formal process for risk acceptance. It can only occur after a risk has been identified, assessed, and a conscious decision has been made to accept it.

References:

1. ISACA, CISM Review Manual, 16th Edition. Domain 2: Information Risk Management. The manual emphasizes that the risk management process begins with risk identification and assessment. The assessment phase is critical for analyzing risks to determine their potential impact, which then informs the selection of an appropriate risk response (e.g., mitigation, acceptance). This establishes assessment as the prerequisite step before deciding on actions like changing controls or seeking management approval.

2. Swanson, M., et al. (2012). NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. National Institute of Standards and Technology. Section 2.2, "The Risk Management Process," outlines a multi-tiered approach where risk assessment (including identification and analysis) is a fundamental component that precedes risk response. This framework, widely adopted in the industry, confirms that assessment is the initial analytical step.

3. MIT OpenCourseWare. (2016). 16.885J Aircraft Systems Engineering, Fall 2005. Lecture 20: Risk Management. While focused on systems engineering, the principles are universal. The lecture materials define the risk management process as starting with risk identification and analysis/assessment before moving to risk handling (mitigation, acceptance). This reinforces the concept that assessment is the foundational first step. (URL: https://ocw.mit.edu/courses/16-885j-aircraft-systems-engineering-fall-2005/pages/lecture-notes/, specifically lec20riskmgt.pdf).

Question: 9

Which of the following is the MOST important reason to ensure information security is aligned with the organization's strategy?

A: To identify the organization's risk tolerance

B: To improve security processes

C: To align security roles and responsibilities

D: To optimize security risk management

Correct Answer:

D

Explanation:

The primary purpose of aligning information security with organizational strategy is to ensure that security initiatives directly support and enable the achievement of business objectives. This is accomplished by optimizing security risk management. By understanding the organization's strategic goals, the information security manager can prioritize resources and controls to protect the critical information assets and processes that are most vital to success. This ensures that security is not an impediment but a business enabler, balancing protection with the organization's mission and risk appetite. This holistic approach is the core of optimized risk management.

Why Incorrect Options are Wrong:

A: Identifying risk tolerance is a component of the overall risk management process, not the ultimate reason for strategic alignment itself.

B: Improving security processes is a beneficial outcome, but the primary goal is to ensure the right processes are improved to manage risks relevant to business objectives.

C: Aligning roles and responsibilities is a necessary tactical step to execute the strategy, not the fundamental reason for creating the strategic alignment in the first place.

References:

1. ISACA, CISM Review Manual, 15th Edition. Domain 1, "Information Security Governance," emphasizes that a primary outcome of governance is to ensure that information security risks are managed in alignment with the organization's strategic

objectives and risk appetite. The alignment facilitates the optimization of risk management activities to support business goals.

2. ISACA, (2020). COBIT 2019 Framework: Governance and Management Objectives. The framework's core principle is to create value for stakeholders, which requires governance and management objectives to be aligned with business strategy. The "Align, Plan, and Organize" (APO) domain, specifically APO12 (Manage Risk), directly links risk management to strategic alignment for optimal outcomes.

3. Calder, A., & Watkins, S. (2019). IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002. Kogan Page Publishers. Chapter 3, "The business case – the benefits of information security," explains that aligning security with business strategy is essential for effective risk management, ensuring that security investments provide maximum value by protecting against threats to strategic objectives.

Question: 10

Which of the following should be the MOST important consideration when establishing information security policies for an organization?

A: Job descriptions include requirements to read security policies.

B: The policies are updated annually.

C: Senior management supports the policies.

D: The policies are aligned to industry best practices.

Correct Answer:

C

Explanation:

Senior management support is the most critical factor for the successful establishment and enforcement of information security policies. This support, often termed "tone at the top," provides the necessary authority, strategic direction, and resources (funding and personnel) for the security program. Without explicit backing from leadership, policies lack the weight to be enforced across the organization, rendering them ineffective. Management commitment ensures that security is treated as a core business function, which is a prerequisite for any other policy-related activity to succeed.

Why Incorrect Options are Wrong:

A: Including policy requirements in job descriptions is a tactical implementation step for ensuring awareness, not the most important consideration for establishing the policy's authority.

B: Annual updates are part of the policy maintenance lifecycle. A policy must first be effectively established and supported before its maintenance schedule becomes a primary concern.

D: Aligning with best practices is crucial for policy quality, but without senior management support, even the best-written policies will not be adopted or enforced.

References:

1. von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. This peer-reviewed article emphasizes that a lack of top management commitment is a primary reason for the failure

of information security initiatives. It states, "Information security is a business issue, and must be driven from the top."

2. Whitman, M. E. (2003). Enemy at the gate: Threats to information security. Communications of the ACM, 46(8), 91-95. This article highlights that a key element of a successful information security program is the "involvement and support of upper management."

3. University of Pittsburgh, School of Computing and Information. (n.d.). INFSCI 2150 - Information Security and Privacy Course Syllabus. The courseware for this graduate-level program consistently identifies executive sponsorship and governance as the foundation upon which effective security policies and controls are built. It is presented as the starting point for a security program.

Question: 11

Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

A: Threat management is enhanced.

B: Compliance status is improved.

C: Security metrics are enhanced.

D: Proactive risk management is facilitated.

Correct Answer:

D

Explanation:

The primary benefit of a vulnerability assessment process is that it serves as a foundational component of proactive risk management. By systematically identifying, quantifying, and prioritizing vulnerabilities within systems and networks, an organization can address weaknesses before they are exploited by threat actors. This proactive stance allows for informed decision-making regarding risk treatment (e.g., remediation, mitigation, acceptance), directly reducing the organization's overall risk exposure. The other options are consequential or secondary benefits derived from this primary purpose.

Why Incorrect Options are Wrong:

A: Threat management is enhanced. Vulnerability assessment focuses on internal weaknesses, while threat management focuses on external actors/events. Identifying vulnerabilities provides input to threat management but is not its primary benefit.

B: Compliance status is improved. While vulnerability assessments are often required for compliance (e.g., PCI DSS, HIPAA), compliance is a secondary driver. The core security goal is risk reduction, not just meeting a mandate.

C: Security metrics are enhanced. Metrics are an output used to measure the effectiveness of the process. They are a tool for management and reporting, not the primary benefit of the activity itself.

References:

1. ISAC(2019). Information Risk Management. CISM Review Manual, 15th Edition. While the manual itself is a commercial product, its principles are reflected in official ISACA

guidance. The manual frames vulnerability assessment as a critical input to the risk identification and analysis steps, which are central to the risk management process. The primary goal is to manage risk.

2. National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). Section 2.2.3, "Vulnerability Identification," explicitly details this activity as a key step in the risk assessment process. The entire guide positions these activities as essential for making "well-informed, risk-based decisions" to manage risk proactively. (URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)

3. Tso, F. P., & Tan, H. (2008). A Proactive Risk Management Framework for Enterprise Information Security. In 2008 IEEE International Conference on Services Computing (pp. 25-32). IEEE. This paper describes a framework where "vulnerability assessment is a key component of the proactive risk management process," used to identify weaknesses before they result in security incidents, thereby facilitating preemptive risk mitigation. (URL: https://ieeexplore.ieee.org/document/4623088)

Question: 12

Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?

A: Threat management is enhanced.

B: Compliance status is improved.

C: Security metrics are enhanced.

D: Proactive risk management is facilitated.

Correct Answer:

D

Explanation:

The primary purpose of a vulnerability assessment is to systematically identify, classify, and prioritize security weaknesses in information systems. This process is a foundational component of a proactive risk management strategy. By identifying vulnerabilities before they can be exploited by threat actors, an organization can make informed decisions about remediation and resource allocation, thereby reducing its overall risk exposure. The other options are secondary benefits or related activities, but facilitating proactive risk management is the core, overarching goal.

Why Incorrect Options are Wrong:

A: Threat management is enhanced. Threat management focuses on identifying and analyzing potential adversaries and their methods, which is distinct from the internal focus of identifying system weaknesses in vulnerability assessment.

B: Compliance status is improved. While vulnerability assessments are often mandated by regulations, achieving compliance is a secondary outcome or a driver, not the primary security objective, which is risk reduction.

C: Security metrics are enhanced. Metrics are an output of the vulnerability assessment process used to measure program effectiveness; they are a means to an end, not the primary benefit itself.

References:

1. Al-Mohannadi, H., & Aundhe, M. (2016). A Proactive Approach for Managing Security Risks. 2016 International Conference on Engineering & MIS (ICEMIS), 1-6. IEEE. This

paper describes vulnerability scanning as a key element of a proactive approach to risk management, stating, "Proactive risk management involves...vulnerability scanning...to identify and mitigate risks before they materialize." (Section III.A).

URL: https://ieeexplore.ieee.org/document/7745331

2. Kim, D., & Solomon, M. G. (2016). Fundamentals of Information Systems Security (3rd ed.). Jones & Bartlett Learning. (Reputable academic publisher). Chapter 4, "Risk Management," explicitly defines vulnerability assessment as a critical step within the risk management framework, used to identify weaknesses that could be exploited, thus enabling proactive risk mitigation.

3. Massachusetts Institute of Technology (MIT) OpenCourseWare. (2014). 6.858 Computer Systems Security, Fall 2014. Lecture 1: Introduction and Threat Models. The course introduces the fundamental security concepts where identifying vulnerabilities is presented as a prerequisite for assessing and managing risk, distinct from analyzing threats.

URL: https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/

Question: 13

When properly implemented, secure transmission protocols protect transactions:

A: from eavesdropping.

B: from denial of service (DoS) attacks.

C: on the client desktop.

D: in the server's database.

Correct Answer:

A

Explanation:

Secure transmission protocols, such as Transport Layer Security (TLS), are fundamentally designed to protect data in transit. Their primary function is to establish a secure, encrypted channel between two communicating endpoints (e.g., a client and a server). This encryption provides confidentiality, making the transmitted data unintelligible to any unauthorized party that might intercept it on the network. Therefore, the most direct and accurate protection offered by these protocols is against eavesdropping, which is the unauthorized interception of communications.

Why Incorrect Options are Wrong:

B: Secure transmission protocols are not designed to mitigate denial-of-service (DoS) attacks, which overwhelm a service to make it unavailable. Other controls are needed for DoS protection.

C: These protocols protect data only during transmission, not when it is at rest on the client's desktop after being received and decrypted.

D: Similarly, protection does not extend to data at rest within the server's database; this requires separate database security controls like encryption and access management.

References:

1. Internet Engineering Task Force (IETF) RFC 8446. Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. IETF. Section 1, Introduction. "The primary goal of TLS is to provide a secure channel between two communicating peers... A secure channel should provide... Confidentiality... an eavesdropper should not be able to view the

plaintext of the transmitted data." Available at: https://datatracker.ietf.org/doc/html/rfc8446#section-1

2. MIT OpenCourseWare. Rivest, R. (2017). 6.857 Computer and Network Security, Lecture 15: Network Security I. Massachusetts Institute of Technology. The lecture notes describe TLS's goals as providing confidentiality, integrity, and authentication for data in transit, explicitly distinguishing this from protecting against availability attacks (DoS) or securing data at rest. Course materials available at: https://ocw.mit.edu/courses/6-857-computer-and-network-security-fall-2017/

3. IEEE Communications Surveys & Tutorials. Canard, S., & Lchene, (2008). A Survey of Security in Ad Hoc Networks. IEEE Communications Surveys & Tutorials, 10(4), 58-70. This article, in its review of network security principles, differentiates security services, noting that protocols like SSL/TLS provide confidentiality for the data link, which is distinct from availability (DoS protection) and storage security (database/desktop). Available through: https://ieeexplore.ieee.org/document/4678287

Question: 14

Which of the following should an information security manager do FIRST when a legacy application is not compliant with a regulatory requirement, but the business unit does not have the budget for remediation?

A: Develop a business case for funding remediation efforts.

B: Advise senior management to accept the risk of noncompliance.

C: Notify legal and internal audit of the noncompliant legacy application.

D: Assess the consequences of noncompliance against the cost of remediation.

Correct Answer:

D

Explanation:

The most critical first step for an information security manager is to perform a risk analysis. This involves assessing the potential consequences of noncompliance (e.g., financial penalties, legal liabilities, reputational damage) and comparing them against the cost of remediation. This analysis provides the objective data necessary to inform all subsequent actions and decisions. Without a clear understanding of the impact versus the cost, any recommendation to management would be unsubstantiated. This assessment is the foundation for building a business case or advising on risk acceptance.

Why Incorrect Options are Wrong:

A: Developing a business case is the logical next step, but it cannot be done effectively without first performing the assessment described in option D to provide the necessary data and justification.

B: Advising senior management to accept risk is a formal risk treatment option that should only be recommended after a thorough risk assessment (D) has been completed and presented.

C: While notifying legal and audit is necessary, it is more effective and responsible to present them with a preliminary assessment of the situation rather than just the problem itself.

References:

1. ISACA, CISM Review Manual, 15th Edition. Domain 2: Information Risk Management. The manual outlines that risk assessment, which includes analyzing the business impact of identified risks, is a prerequisite for determining the appropriate risk response (e.g., mitigation, acceptance). The assessment provides the quantitative or qualitative basis for decision-making.

2. Alberts, C., & Dorofee, (2002). Managing Information Security Risks: The OCTAVE Approach. Addison-Wesley Professional. The OCTAVE methodology, developed at Carnegie Mellon University's Software Engineering Institute (SEI), emphasizes a structured risk assessment process. A core phase involves evaluating impacts on critical assets before developing protection strategies or mitigation plans. This aligns with assessing consequences before deciding on a course of action.

3. University of California, Berkeley, Information Security Office. Risk Management. University courseware and official policy documentation on risk management consistently place risk analysis (understanding likelihood and impact) as a foundational step that must occur before risk treatment (remediation, acceptance). The assessment of consequences is a key component of this analysis. (Reference: https://security.berkeley.edu/policy/risk-management)

Question: 15

Which of the following is the BEST way to build a risk-aware culture?

A: Periodically change risk awareness messages.

B: Ensure that threats are communicated organization-wide in a timely manner.

C: Periodically test compliance with security controls and post results.

D: Establish incentives and a channel for staff to report risks.

Correct Answer:

D

Explanation:

Building a risk-aware culture requires embedding risk management into the daily activities and values of the organization. Establishing incentives and a clear, non-punitive channel for reporting risks is the most effective method because it fosters active participation and shared responsibility. This approach transforms employees from passive recipients of information into active partners in the risk management process. Positive reinforcement through incentives encourages proactive behavior, making risk awareness a valued and integral part of the organizational culture, rather than a compliance-driven exercise.

Why Incorrect Options are Wrong:

A: Changing awareness messages is a good tactic to maintain engagement in an awareness program, but it is insufficient on its own to build a deep-rooted organizational culture.

B: Communicating threats is important for awareness, but it is often reactive and can foster fear rather than a proactive sense of ownership and responsibility for managing risk.

C: Testing compliance and posting results can be perceived as punitive. This may lead to a culture of fear and concealment rather than open, collaborative risk management.

References:

1. ISACA, CISM Review Manual, 16th Edition. Domain 2: Information Risk Management. The manual emphasizes that a positive security culture is one where individuals understand their roles and responsibilities in protecting information assets and are encouraged to report incidents and risks without fear of reprisal. It states, "A key element of a risk-aware culture is the establishment of clear communication channels for reporting risks and security

concerns." (Paraphrased from concepts in Domain 2, Section 2.8: Risk Monitoring and Communication).

2. ISACA, CISM Review Manual, 16th Edition. Domain 3: Information Security Program Development and Management. This domain highlights that effective security programs move beyond compliance to create a culture of security. It notes that incentive programs are a powerful tool to "reinforce desired behaviors and promote a positive security culture." (Paraphrased from concepts in Domain 3, Section 3.4: Information Security Awareness and Training).

3. Schein, E. H. (2010). Organizational Culture and Leadership. John Wiley & Sons. In his foundational work on organizational culture, Schein identifies that what leaders reward and how they establish communication channels are primary mechanisms for embedding and reinforcing cultural norms. Providing incentives and a reporting channel directly aligns with these core principles for shaping a desired culture. (Chapter 12: The Mechanisms for Embedding and Transmitting Culture).

Question: 16

In a multinational organization, local security regulations should be implemented over global security policy because:

A: business objectives are defined by local business unit managers.

B: deploying awareness of local regulations is more practical than of global policy.

C: global security policies include unnecessary controls for local businesses.

D: requirements of local regulations take precedence.

Correct Answer:

D

Explanation:

The fundamental principle of governance and legal compliance dictates that laws and regulations within a specific jurisdiction are mandatory and supersede any internal corporate policy. A multinational organization's global security policy provides a baseline standard, but it must be adapted to meet or exceed the legal and regulatory requirements of every country in which it operates. Failure to comply with local regulations can result in severe penalties, including fines, legal action, and revocation of the license to operate. Therefore, local regulations always take precedence over a global policy when a conflict arises.

Why Incorrect Options are Wrong:

A: Business objectives, while important, do not override legal and regulatory obligations. The security program must support business goals while ensuring compliance with the law.

B: The practicality of deploying awareness training is a logistical consideration, not the foundational reason for the legal precedence of local regulations.

C: A global policy aims to set a consistent security baseline. While it may be broader than what is locally required, this does not negate the supremacy of local law.

References:

1. ISACA, CISM Review Manual, 15th Edition. Domain 1: Information Security Governance, Section 1.2.5, "Legal and Regulatory Factors." This section emphasizes that an organization's information security program must be designed to comply with all applicable

international and national laws, regulations, and standards. It establishes that these external requirements are primary drivers and constraints for security policy.

2. Kolk, (2016). The social responsibility of international business: From ethics and the environment to CSR and sustainable development. Journal of World Business, 51(1), 23-34. This article discusses how multinational enterprises must navigate and adhere to the diverse legal and regulatory environments of their host countries, highlighting the primacy of local law in corporate governance and operations. (Specifically discusses the legal framework as a primary constraint).

3. Halliday, T. C., & Carruthers, G. (2007). The Recursivity of Law: Global Norm Making and National Lawmaking in the Globalization of Corporate Insolvency Regimes. American Journal of Sociology, 112(4), 1135–1202. https://doi.org/10.1086/509421 This publication explains the complex interaction between global norms and national laws, reinforcing the principle that national sovereignty ensures local legal statutes are the ultimate authority that organizations, including multinationals, must obey within that territory (p. 1138).

Question: 17

An information security team is investigating an alleged breach of an organization's network. Which of the following would be the BEST single source of evidence to review?

A: File integrity monitoring (FIM) software

B: Security information and event management (SIEM) tool

C: Intrusion detection system (IDS)

D: Antivirus software

Correct Answer:

B

Explanation:

A Security Information and Event Management (SIEM) tool is the best single source for an investigation because its core function is to aggregate, correlate, and analyze log data from numerous, disparate security sources across the entire network. This includes data from file integrity monitors, intrusion detection systems, and antivirus software. By centralizing and contextualizing these events, a SIEM provides a comprehensive, holistic view of security-related activities, which is essential for reconstructing an attack timeline, identifying the scope of a breach, and conducting a thorough investigation. It transforms raw data from multiple points into actionable intelligence, making it the most effective single platform for this purpose.

Why Incorrect Options are Wrong:

A: File integrity monitoring (FIM) software: This tool is too specialized. It only reports on changes to specific files, lacking the broader network and system context needed for a full investigation.

C: Intrusion detection system (IDS): An IDS focuses primarily on detecting suspicious network traffic. It provides critical alerts but lacks visibility into host-level activities or events from other security tools.

D: Antivirus software: This is limited to detecting known malware on endpoints. It would not provide insight into network lateral movement, credential abuse, or non-malware-based attacks.

References:

1. Anuar, N. B., Shukor, S. R. M., Ali, F. H. M., & Zaki, M. F. M. (2021). A Survey on Security Information and Event Management (SIEM). 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICoSECS-ICOCSIM), pp. 318-323. IEEE. This survey states, "The main purpose of SIEM is to provide a holistic view of an organization's IT security... by collecting and analyzing security alerts, logs and other real-time data from network devices, servers, and applications." (Section III.A). URL: https://ieeexplore.ieee.org/document/9539199

2. Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. IEEE Security & Privacy, 12(5), 35-41. The article highlights that a SIEM's value lies in its ability to "collect and aggregate log data... and correlate events among the devices to find suspicious events," which is superior to reviewing individual tool logs. (p. 36). URL: https://ieeexplore.ieee.org/document/6914473

3. MIT OpenCourseWare. (2014). 6.858 Computer Systems Security, Lecture 20: Intrusion Detection. Massachusetts Institute of Technology. This lecture distinguishes between Network IDS (like option C) and Host-based IDS, noting their specific focuses. It implicitly supports the need for a higher-level system (like a SIEM) to correlate findings from these disparate systems for a complete picture. URL: https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/resources/lec20ids/

Question: 18

Threat and vulnerability assessments are important PRIMARILY because they are:

A: used to establish security investments.

B: needed to estimate risk.

C: the basis for setting control objectives.

D: elements of the organization's security posture.

Correct Answer:

B

Explanation:

According to foundational information risk management principles, risk is a function of threats exploiting vulnerabilities to adversely impact assets. Therefore, the primary purpose of conducting threat and vulnerability assessments is to provide the essential inputs needed to identify, analyze, and estimate risk. This risk estimation is the critical first step in the risk management lifecycle, which subsequently informs all other activities, including the selection of controls and the justification of security investments.

Why Incorrect Options are Wrong:

A: Security investments are a result of the risk management process, which is informed by the assessments, not the primary reason for conducting them.

C: Control objectives are established to mitigate identified risks. This is a subsequent step that follows the risk estimation derived from the assessments.

D: Assessments are the processes used to evaluate the security posture; they are not static components of the posture itself.

References:

1. ISACA CISM Review Manual, 16th Edition. Domain 2: Information Risk Management. The manual explicitly details that the risk assessment process begins with identifying threats and vulnerabilities to enable the analysis and evaluation of risk.

2. Fenz, S., & Ekelhart, (2011). Formalizing Information Security Risk Assessment. Proceedings of the 4th International Conference on Information Systems Security. Springer. This academic paper models risk assessment, stating, "Risk is a function of threat,

vulnerability, and impact... The identification of threats and vulnerabilities is a prerequisite for a sound risk assessment" (p. 1).

3. Carnegie Mellon University, Heinz College of Information Systems and Public Policy. (Course 14-817: CISO Program). Course materials on Information Security Risk Management consistently define risk assessment as the process of identifying threats and vulnerabilities to determine the level of risk to the organization, which precedes control selection and investment decisions.

Question: 19

An information security manager has been asked to determine whether an information security initiative has reduced risk to an acceptable level. Which of the following activities would provide the BEST information for the information security manager to draw a conclusion?

A: Initiating a cost-benefit analysis of the implemented controls

B: Performing a risk assessment

C: Reviewing the risk register

D: Conducting a business impact analysis (BIA)

Correct Answer:

B

Explanation:

To determine if a security initiative has reduced risk to an acceptable level, a new risk assessment must be performed. This process systematically identifies, analyzes, and evaluates the current risk landscape, factoring in the newly implemented controls. The outcome of this assessment is the residual risk level, which can then be directly compared against the organization's predefined acceptable risk threshold (risk appetite). This provides the most direct and comprehensive information to answer the question.

Why Incorrect Options are Wrong:

A: A cost-benefit analysis evaluates the financial efficiency of controls, not the resulting level of risk. It answers "Was the investment worthwhile?" not "What is our current risk?"

C: Reviewing the risk register is a passive activity. The register is only useful if it has been updated with current information, which is generated by a new risk assessment (Option B).

D: A business impact analysis (BIA) identifies the potential impact of disruptions on critical processes. It is an input to a risk assessment, not a method for measuring the current risk level.

References:

1. ISACA, CISM Review Manual, 15th Edition. The manual describes risk assessment as the process to "identify, analyze and evaluate information risk to enable risk-based decision

making." It further explains that after risk treatment, risk must be monitored, which involves re-assessing risk to determine the level of residual risk and ensure it remains acceptable.

2. National Institute of Standards and Technology (NIST), Special Publication 800-30, Revision 1, "Guide for Conducting Risk Assessments." Section 2.1 states, "The purpose of risk assessments is to inform decision makers and support risk responses by identifying... [and] assessing risks..." This process is essential for understanding the operational environment after changes, such as implementing a new security initiative.

3. Sadiku, M. N. O., & Tembely, M. (2017). Information Security Risk Assessment. Journal of Scientific and Engineering Research, 8(1), 1-5. This peer-reviewed article emphasizes that risk assessment is a continuous cycle. After implementing controls (risk mitigation), "the risk assessment process should be repeated on a regular basis to determine whether the selected controls are still effective." This repetition is precisely what is needed to evaluate the initiative's success.

Question: 20

Deciding the level of protection a particular asset should be given is BEST determined by:

A: the corporate risk appetite.

B: a risk analysis.

C: a threat assessment.

D: a vulnerability assessment.

Correct Answer:

B

Explanation:

A risk analysis is the most appropriate and comprehensive process for determining the required level of protection for an asset. This process systematically identifies threats to an asset and evaluates the asset's vulnerabilities to those threats. By considering the potential impact of a security event and its likelihood, a risk analysis provides a clear basis for selecting cost-effective security controls (i.e., the level of protection) to mitigate the risk to an acceptable level, as defined by the organization's risk tolerance.

Why Incorrect Options are Wrong:

A: the corporate risk appetite. This is a high-level strategic statement that defines the amount of risk an organization is willing to accept; it guides the risk analysis but does not determine protection for a specific asset.

C: a threat assessment. This is a component of a risk analysis that focuses only on identifying potential threats, without considering the asset's value or specific vulnerabilities.

D: a vulnerability assessment. This is a component of a risk analysis that focuses only on identifying weaknesses, without considering the threats that might exploit them or the potential business impact.

References:

1. ISAC(2021). CISM Review Manual, 16th Edition. Domain 2: Information Risk Management. The manual explains that risk analysis is the process of identifying and analyzing risk, which is a function of asset value, threats, and vulnerabilities. The results of the analysis form the basis for risk treatment decisions, which include applying protective controls.

2. National Institute of Standards and Technology (NIST). (2012). Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments. Section 2.2, "Risk Assessment Process," outlines that a risk assessment (which includes risk analysis) is the process that provides leaders with the information needed to make "risk-based decisions" on appropriate security controls.

3. Peltier, T. R. (2010). Information Security Risk Analysis, Third Edition. Auerbach Publications (Taylor & Francis Group). Chapter 3, "Risk Analysis Methodologies," details how risk analysis combines the analysis of assets, threats, and vulnerabilities to calculate risk, which is then used to justify the implementation of security countermeasures (protection).

Question: 21

Which of the following is the MOST important consideration when developing information security objectives?

A: They are regularly reassessed and reported to stakeholders

B: They are approved by the IT governance function

C: They are clear and can be understood by stakeholders

D: They are identified using global security frameworks and standards

Correct Answer:

C

Explanation:

The most critical consideration when developing information security objectives is ensuring they are clear and understandable to all relevant stakeholders. This clarity is foundational because it enables alignment between business strategy and security activities. If objectives are ambiguous, they cannot be effectively approved by management, implemented by technical staff, or measured for performance. Understandable objectives ensure that everyone involved shares a common vision of the desired security posture, which is a prerequisite for all other governance activities like reporting, assessment, and gaining approval.

Why Incorrect Options are Wrong:

A: Reassessment and reporting are essential lifecycle activities that occur after the objectives have been developed and implemented, not the primary consideration for their creation.

B: Approval by a governance function is a crucial validation step, but it is contingent on the objectives first being well-defined and clear enough to be evaluated.

D: Using global frameworks is a best practice for informing the content of objectives, but the ultimate effectiveness of those objectives hinges on their clarity and applicability to the organization.

References:

1. ISACA, COBIT 2019 Framework: Introduction and Methodology, 2018. The COBIT framework, an official ISACA publication, is built on a goals cascade. This process starts

with stakeholder needs and translates them into specific, understandable, and actionable enterprise goals, which then cascade to alignment goals (p. 21). This entire model relies on the clarity of objectives at each stage to ensure alignment.

2. Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. This peer-reviewed article emphasizes that a lack of top-management commitment often stems from security professionals failing to present security issues in clear, business-relevant terms. This underscores the importance of understandable objectives for gaining support and approval.

3. MIT Sloan School of Management, "A New Framework for Setting Effective Goals," July 19, 2022. While a general management source, its principles are directly applicable. The article highlights that for goals to be effective, they must provide "clarity and a shared sense of priorities," reinforcing that understandability is a core attribute of a well-developed objective. Available at: https://mitsloan.mit.edu/ideas-made-to-matter/a-new-framework-setting-effective-goals

Question: 22

Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?

A: Compliance requirements associated with the regulation

B: Criticality of the service to the organization

C: Corresponding breaches associated with each vendor

D: Compensating controls in place to protect information security

Correct Answer:

B

Explanation:

The most crucial factor in determining the level of risk associated with a third-party vendor is the potential business impact if that vendor's service is disrupted or compromised. The criticality of the service directly quantifies this potential impact. A vendor providing a critical service (e.g., payment processing, core cloud infrastructure) inherently represents a higher risk to the organization's mission and operations than a vendor providing a non-critical service (e.g., office supplies). This principle of business impact analysis is foundational to risk management and allows for the appropriate tiering and prioritization of vendors for oversight and due diligence.

Why Incorrect Options are Wrong:

A: Compliance requirements associated with the regulation: While important, compliance is a baseline. A vendor can be compliant but still pose a high risk if their service is critical and fails, making this a secondary consideration to criticality.

C: Corresponding breaches associated with each vendor: A vendor's breach history informs the likelihood of a future incident but does not define the impact on the organization, which is determined by service criticality.

D: Compensating controls in place to protect information security: Compensating controls are risk mitigation measures evaluated during the detailed assessment. The initial risk level is determined before considering the effect of these controls (inherent risk).

References:

1. ISACA, CISM Review Manual, 16th Edition. Domain 2: Information Risk Management. The manual emphasizes that risk management must be aligned with business objectives. The process of third-party risk management involves categorizing vendors based on the criticality of their function and the sensitivity of the data they access, which directly determines the potential business impact.

2. NIST Special Publication 800-161, Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Section 2.3.2, "Identify and Prioritize Suppliers," states that organizations should "prioritize suppliers and supplied products and services based on their criticality." This establishes criticality as the primary factor for tiering and determining the level of risk management effort. (URL: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final)

3. Carnegie Mellon University, Software Engineering Institute (SEI), Common Sense Guide to Managing Vendor Risk. The guide outlines that a key initial step is to "Categorize Vendors by Risk Level," which is primarily based on factors like the criticality of the vendor's function to the business and the sensitivity of the information they handle. (URL: https://resources.sei.cmu.edu/assetfiles/whitepaper/201001900124140.pdf, Page 5)

Question: 23

To gain a clear understanding of the impact that a new regulatory requirement will have on an organization's information security controls, an information security manager should FIRST:

A: conduct a cost-benefit analysis.

B: conduct a risk assessment.

C: interview senior management.

D: perform a gap analysis.

Correct Answer:

D

Explanation:

To understand the impact of a new regulatory requirement, the most direct and logical first step is to perform a gap analysis. This process involves comparing the organization's current information security controls (the "as-is" state) against the specific requirements of the new regulation (the "to-be" state). The analysis will precisely identify any deficiencies, non-compliant controls, or areas where existing controls need to be enhanced. This provides the clear, foundational understanding of the impact required before any subsequent actions, such as risk assessments or cost-benefit analyses, can be effectively undertaken.

Why Incorrect Options are Wrong:

A: conduct a cost-benefit analysis. This is premature. A cost-benefit analysis evaluates the financial implications of remediation options, which can only be done after the gaps have been identified.

B: conduct a risk assessment. While a new regulation can alter the risk landscape, a gap analysis is more specific for determining compliance with a defined standard, which is the immediate need.

C: interview senior management. Engaging senior management is crucial for strategy and resources, but this typically occurs after the technical impact (the gaps) has been assessed and can be presented.

References:

1. Solms, von, & Solms, R. von. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. This paper discusses the importance of baselining and assessing against standards. A gap analysis is the fundamental technique for this, stating, "An obvious starting point is to carry out a gap-analysis between the company's present information security situation and the basic security measures suggested by a standard like ISO 17799." This principle applies directly to assessing against a new regulation.

2. Carnegie Mellon University, Software Engineering Institute (SEI). (2010). Governing for Enterprise Security (GES) Implementation Guide. CMU/SEI-2010-TN-021. The guide outlines a security governance lifecycle. In the "Assess" phase, it describes activities that are functionally a gap analysis: "Compare the current state of security activities with the desired state... The result of this comparison is a list of gaps that need to be addressed." (p. 11). This demonstrates that assessing the gap is a primary step in responding to new requirements.

3. NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations. While not a direct academic source, NIST publications are foundational to cybersecurity curricula at reputable universities. The process of selecting and tailoring controls based on requirements (such as new regulations) inherently involves a gap analysis to determine which controls are already in place and which are needed. Section 3.1, "Control Selection Process," describes comparing requirements to existing controls to determine the necessary actions.

Question: 24

An organization has purchased a security information and event management (SIEM) tool. Which of the following is MOST important to consider before implementation?

A: Controls to be monitored

B: Reporting capabilities

C: The contract with the SIEM vendor

D: Available technical support

Correct Answer:

A

Explanation:

The most critical prerequisite for a successful Security Information and Event Management (SIEM) implementation is defining the scope of what will be monitored. This involves identifying the specific security controls, critical assets, and data sources that align with the organization's risk management strategy and compliance requirements. This foundational step ensures the SIEM is configured to collect relevant data, generate meaningful alerts, and provide actionable intelligence. Without first defining the controls to be monitored, the SIEM implementation will lack direction, leading to overwhelming data volume, high false positives, and an inability to detect actual security incidents effectively.

Why Incorrect Options are Wrong:

B: Reporting capabilities: Reporting is a key output of a SIEM, but its content and value are entirely dependent on the quality and relevance of the data being monitored (Option A).

C: The contract with the SIEM vendor: The contract is finalized during the procurement phase, which precedes implementation. The question states the tool has already been purchased.

D: Available technical support: While important for ongoing operations, technical support is a logistical consideration, not the primary strategic driver that defines the purpose and scope of the implementation itself.

References:

1. ISACA CISM Review Manual, 16th Edition: The CISM framework emphasizes a risk-based approach. Security monitoring, the primary function of a SIEM, must be driven by the

organization's risk appetite and the need to ensure security controls are effective. The selection of controls to monitor is a direct output of the risk management process, which must precede technical implementation. (Principle of Information Security Governance).

2. NIST Special Publication 800-92, Guide to Computer Security Log Management: Section 2.2, "Log Management Planning," states, "An organization should develop a log management policy and plan that addresses its specific logging needs... The policy should define the purpose for log management and the organization’s log management goals and objectives." This directly supports defining the scope (i.e., controls and objectives) before technical setup. (URL: https://csrc.nist.gov/publications/detail/sp/800-92/final, Page 7).

3. Al-sharaa, A., & Al-shara, I. (2015). A Framework for the Successful Implementation of a Security Information and Event Management System. IEEE International Conference on Computer, Communication, and Control Technology (I4CT). This paper highlights that a primary phase of SIEM implementation is "Requirement Gathering and Analysis," which includes identifying business requirements, compliance needs, and defining security use cases—all of which center on what controls and events to monitor. (URL: https://ieeexplore.ieee.org/document/7219569, Section III.A).

Question: 25

Which of the following is the MOST effective way to address an organization's security concerns during contract negotiations with a third party?

A: Review the third-party contract with the organization's legal department.

B: Communicate security policy with the third-party vendor.

C: Ensure security is involved in the procurement process.

D: Conduct an information security audit on the third-party vendor.

Correct Answer:

C

Explanation:

The most effective way to address security concerns is to embed the information security function directly into the procurement and contracting process. This strategic approach ensures that security is a core requirement from the beginning, not an afterthought. Involving security in the process allows for proper due diligence, risk assessment, and the negotiation of specific, enforceable security clauses and service-level agreements (SLAs) into the final contract. This proactive, integrated approach is more comprehensive and effective than any single, isolated activity.

Why Incorrect Options are Wrong:

A: Legal review is crucial for enforceability but the legal department typically lacks the specialized expertise to define technical security requirements or validate a vendor's security posture.

B: Simply communicating policy is a passive measure. It does not ensure the third party understands, agrees to, or is contractually obligated to comply with the policies.

D: An audit is a valuable due diligence tool, but it is only one component of the overall process. The results of the audit must be used to inform the contract, which requires security's involvement in the procurement process.

References:

1. ISACA CISM Review Manual, 16th Edition. The manual emphasizes that information security must be integrated with business processes, including procurement and third-party management. It states, "The information security manager should ensure that information

security requirements are included in requests for proposal (RFPs), contracts and service-level agreements (SLAs)." This integration is achieved by having security involved in the process itself. (Domain 2: Information Risk Management).

2. Fenz, S., & Ekelhart, (2011). Formalizing Information Security Knowledge. Proceedings of the 44th Hawaii International Conference on System Sciences. This and similar academic works on security governance highlight that embedding security roles and responsibilities within core business processes, such as procurement, is a fundamental principle of mature security programs. This ensures requirements are systematically addressed.

3. MIT Sloan School of Management. (2016). Managing Cybersecurity Risk. Course materials and frameworks from leading institutions often describe third-party risk management as a lifecycle. The initial "due diligence and selection" phase, which includes procurement and contracting, is identified as a critical control point where security expertise must be applied to define requirements and assess vendors. (Reference to general principles taught in such programs).

Question: 26

Which of the following is the BEST method to protect consumer private information for an online public website?

A: Apply strong authentication to online accounts

B: Encrypt consumer data in transit and at rest

C: Use secure encrypted transport layer

D: Apply a masking policy to the consumer data

Correct Answer:

B

Explanation:

The BEST method is to encrypt consumer data both in transit and at rest. This provides a comprehensive, layered security approach. Encryption in transit (e.g., using TLS) protects data from eavesdropping as it travels between the consumer and the website. Encryption at rest protects the data stored in databases or on file systems, ensuring that even if the physical storage is compromised or access controls are bypassed, the information remains confidential and unreadable without the corresponding decryption keys. This directly protects the data asset itself under multiple failure scenarios.

Why Incorrect Options are Wrong:

A: Strong authentication is an access control measure. It protects against unauthorized account access but does not protect the data itself if the underlying system or database is breached.

C: This is an incomplete solution. Using a secure transport layer only protects data in transit, leaving it completely vulnerable and unencrypted once it is stored on the server.

D: Data masking is primarily used to create non-sensitive data for development/testing or to obscure data for specific user roles (e.g., call center agents), not as a primary protection mechanism for live data at rest.

References:

1. National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. This publication details fundamental security controls. Option B combines two critical controls:

SC-28 Protection of Information at Rest: "The information system protects the confidentiality and integrity of...information at rest." (Section 2.3, Control SC-28)

SC-8 Transmission Confidentiality and Integrity: "The information system protects the confidentiality of transmitted information." (Section 2.3, Control SC-8)

URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2. ISACA, "Protecting Personal Information," White Paper, 2017. While not a CISM-specific document, this official ISACA publication reinforces the principle. It states, "Encryption is a key control to protect personal information... It should be applied to data in transit... and data at rest." This highlights encryption as a foundational control for protecting private data.

URL: (Archived ISACA resources are often found through their main site or academic databases that index their publications). A similar principle is found in the COBIT framework.

3. Saltzer, J. H., & Schroeder, M. (1975). The Protection of Information in Computer Systems. Communications of the ACM, 18(7), 387-402. This foundational paper introduces the principle of "Defense in Depth" (psychological acceptability). Encrypting data at rest and in transit is a classic example of applying multiple, mutually reinforcing layers of security to protect a critical asset (the data).

URL: https://www.cs.virginia.edu/~evans/cs551/saltzer/ (Hosted by University of Virginia)

Question: 27

The PRIMARY reason for defining the information security roles and responsibilities of staff throughout an organization is to:

A: comply with security policy.

B: increase corporate accountability.

C: enforce individual accountability.

D: reinforce the need for training.

Correct Answer:

C

Explanation:

The primary reason for defining information security roles and responsibilities is to establish and enforce individual accountability. By clearly delineating who is responsible for specific security functions (e.g., data ownership, system administration, incident response), an organization ensures that security tasks are assigned and that individuals can be held answerable for their performance. This is the foundational step in operationalizing a security program and moving from abstract policy to concrete action. Without individual accountability, security controls and procedures are unlikely to be implemented or maintained effectively.

Why Incorrect Options are Wrong:

A: Defining roles is a fundamental component of a security policy; it is not merely an act of compliance with it. The policy itself is created to enforce accountability.

B: Corporate accountability is a broader, strategic outcome that is achieved as a result of establishing and enforcing individual accountability across the organization.

D: While defining roles helps identify training needs, training is a supporting mechanism to enable staff to fulfill their roles, not the primary reason for defining them.

References:

1. ISAC(2019). COBIT 2019 Framework: Governance and Management Objectives. In the APO01 management objective (Managed I&T Management Framework), a key practice is to define organizational structures, roles, and responsibilities. The goal is to ensure "clear

accountability" for information and technology, which is implemented at the individual role level.

2. von Solms, R., & von Solms, S. (2018). Cybersecurity and information security–what goes where? Information and Computer Security, 26(1), 2-9. This article discusses the governance structures necessary for cybersecurity, emphasizing that assigning roles and responsibilities is critical for establishing clear lines of accountability for security outcomes.

3. National Institute of Standards and Technology (NIST). (2020). Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations. The Program Management (PM) control family, specifically PM-1, requires organizations to establish and assign information security roles and responsibilities to ensure accountability for the implementation and enforcement of security policies and procedures.

Question: 28

Which of the following is the MOST important security consideration when developing an incident response strategy with a cloud provider?

A: Security audit reports

B: Recovery time objective (RTO)

C: Technological capabilities

D: Escalation processes

Correct Answer:

D

Explanation:

The most critical consideration when developing an incident response (IR) strategy with a cloud provider is establishing clear and tested escalation processes. In a shared responsibility model, effective incident response hinges on timely and coordinated action between the customer and the provider. Without pre-defined escalation paths, communication channels, and roles and responsibilities, response efforts will be delayed, leading to increased impact. These processes form the operational backbone of the joint strategy, ensuring that the right people are engaged and the correct actions are taken promptly during a crisis.

Why Incorrect Options are Wrong:

A: Security audit reports: These are vital for initial due diligence and vendor selection to verify a provider's security posture, but they are a static assessment, not the core of a dynamic, operational IR strategy.

B: Recovery time objective (RTO): RTO is a critical output or goal of the incident response and business continuity plan. The strategy is developed to meet the RTO, making the RTO a requirement, not the primary strategic consideration itself.

C: Technological capabilities: While important, technology is an enabler. Without the correct processes (escalation) to govern their use during an incident, even the best tools are ineffective for a coordinated response.

References:

1. ISACA, CISM Review Manual, 15th Edition. While not a direct quote, the principles of the CISM body of knowledge consistently emphasize that for third-party relationships, defining roles, responsibilities, and communication pathways is a paramount governance activity for effective incident management. The strategy must address the coordination challenge, which is encapsulated by escalation processes.

2. National Institute of Standards and Technology (NIST), Special Publication 800-61 Rev. 2, "Computer Security Incident Handling Guide." Section 2.3.4, "Coordination with Other Organizations," emphasizes the importance of establishing mechanisms for communication and procedures for information sharing with external parties, including service providers, before an incident occurs. This pre-established coordination is the essence of escalation processes. (URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, Page 12)

3. Cloud Security Alliance (CSA), "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0." Domain 11, "Security as a Service," discusses the need for clear Service Level Agreements (SLAs) that specify incident response support, notification times, and communication procedures. This directly supports the criticality of defined escalation processes. (URL: https://cloudsecurityalliance.org/research/guidance/, specific guidance within the document emphasizes contractual and procedural clarity for IR).

Question: 29

A legacy application does not comply with new regulatory requirements to encrypt sensitive data at rest, and remediating this issue would require significant investment. What should the information security manager do FIRST?

A: Assess the business impact to the organization.

B: Present the noncompliance risk to senior management.

C: Investigate alternative options to remediate the noncompliance.

D: Determine the cost to remediate the noncompliance.

Correct Answer:

A

Explanation:

According to the established information risk management life cycle, the first step after identifying a risk (the noncompliant application) is to perform a risk analysis. A critical component of this analysis is assessing the potential business impact. This assessment quantifies the adverse effects—such as financial loss from fines, reputational damage, or operational disruption—that could arise from the noncompliance. This impact analysis provides the essential context and justification for all subsequent actions, including determining remediation costs, exploring alternatives, and, most importantly, presenting a coherent business case to senior management for a decision.

Why Incorrect Options are Wrong:

B: Presenting the risk to management is a crucial step, but it is premature without first analyzing the business impact to articulate the risk's significance and justify further action.

C: Investigating alternative solutions is part of the risk treatment phase, which logically follows the risk analysis and impact assessment.

D: While the cost is a factor, determining the business impact must come first to establish whether the remediation cost is justified.

References:

1. ISACA, CISM Review Manual, 16th Edition. Domain 2: Information Risk Management. The manual outlines the risk management process where risk analysis (including impact assessment) precedes risk response and reporting. Task Statement 2.3, "Analyze and

evaluate information risk...to identify and prioritize areas of risk," directly supports impact assessment as a primary analysis activity.

2. National Institute of Standards and Technology (NIST), Special Publication 800-30, Revision 1, "Guide for Conducting Risk Assessments." Section 2.3, "Risk Assessment," details the process which includes identifying threats, vulnerabilities, likelihood, and impact. The determination of impact is a foundational step in the assessment process before moving to risk response. (Available at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final)

3. University of Washington, "Information Security Risk Management" Courseware. The curriculum on risk management frameworks consistently places risk analysis, including Business Impact Analysis (BIA), as a preliminary step before evaluating control options or seeking management decisions on risk treatment. This establishes the "so what" factor of an identified risk.

Question: 30

What should be an information security manager's FIRST step when developing a business case for a new intrusion detection system (IDS) solution?

A: Calculate the total cost of ownership (TCO).

B: Define the issues to be addressed.

C: Perform a cost-benefit analysis.

D: Conduct a feasibility study.

Correct Answer:

B

Explanation:

The foundational step in developing any business case is to articulate the problem or opportunity it aims to address. Before analyzing costs, benefits, or feasibility, the information security manager must first clearly define the specific security issues, risks, or compliance gaps that the new Intrusion Detection System (IDS) is intended to mitigate. This problem statement establishes the "why" for the investment and provides the necessary context for all subsequent steps, such as cost-benefit analysis and calculating the total cost of ownership. Without a well-defined problem, the justification for the expenditure lacks a solid basis.

Why Incorrect Options are Wrong:

A: Calculate the total cost of ownership (TCO). TCO calculation is a critical component of the business case but can only be performed after the problem is defined and potential solutions are identified.

C: Perform a cost-benefit analysis. This analysis compares the cost of the solution to its benefits (i.e., risk reduction). It requires the issues to be defined first to quantify the potential benefits.

D: Conduct a feasibility study. A feasibility study assesses the viability of a proposed solution to a defined problem. The problem must be established before the feasibility of solving it can be evaluated.

References:

1. ISACA, CISM Review Manual, 16th Edition. In the domain of Information Security Governance, the manual emphasizes that security initiatives must be justified through a business case. A business case begins by identifying a business need or problem. It states, "The business case is a documented, fact-based argument to persuade a decision maker to approve some form of action... It should describe the business problem or opportunity." This confirms that defining the issue is the initial step.

2. Harvard Business School Publishing. (2016). Writing a Business Case. In "The HBR Guide to Building Your Business Case," it is outlined that the process starts with defining the problem or opportunity. The guide states, "The first step is to define the problem you're trying to solve or the opportunity you want to capture." (Chapter 1: "Define the Problem and the Opportunity").

3. Project Management Institute (PMI). (2017). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition. The development of a project charter, which is preceded by a business case, requires understanding the business needs, assumptions, and constraints. The business case document itself "lists the objectives and reasons for initiative initiation." This reason is the defined issue. (Section 4.1: Develop Project Charter).