

EC-COUNCIL.712-50.v2026-04-06.q272

Exam Code:	712-50
Exam Name:	EC-Council Certified CISO (CCISO)
Certification Provider:	EC-COUNCIL
Free Question Number:	272
Version:	v2026-04-06
# of views:	102
# of Questions views:	2721
https://www.freecram.net/torrent/EC-COUNCIL.712-50.v2026-04-06.q272.html	

NEW QUESTION: 1

The effectiveness of an audit is measured by?

- A. The number of actionable items in the recommendations
- B. How it exposes the risk tolerance of the company
- C. How the recommendations directly support the goals of the company
- D. The number of security controls the company has in use

Answer: (SHOW ANSWER)

Measuring Audit Effectiveness:

* Audits are effective when their recommendations align with and directly contribute to achieving organizational goals.

Value-Driven Recommendations:

* The audit should identify actionable improvements that enhance security while supporting the company's strategic objectives.

Supporting Reference:

* CCISO emphasizes aligning audit recommendations with business goals to ensure their relevance and impact on organizational success.

NEW QUESTION: 2

Which of the following is the BEST security control for reducing the threat of phishing attacks?

- A. Create a data loss prevention capability
- B. Security awareness and training
- C. Implement antivirus within the email system
- D. Increase helpdesk staff

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program identifies security awareness and training as the most effective control against phishing because phishing targets human behavior, not technical flaws.

While antivirus and DLP tools (Options A and C) provide supporting defenses, CCISO materials emphasize that informed users are the primary defense layer. Increasing helpdesk staff (Option D) is reactive, not preventive.

Therefore, Option B is correct.

NEW QUESTION: 3

Which of the following is the MAIN security concern for public cloud computing?

- A. Unable to control physical access to the servers
- B. Unable to track log on activity
- C. Unable to run anti-virus scans
- D. Unable to patch systems as needed

Answer: ([SHOW ANSWER](#))

Cloud Security Concerns

Public cloud computing environments present unique challenges. The most significant concern stems from the lack of direct physical control over server infrastructure. As these servers are managed and owned by third-party providers, organizations cannot implement or enforce their physical security measures. This concern is frequently emphasized in EC-Council's CISO guidance as it directly affects the CIA (Confidentiality, Integrity, Availability) triad.

Impact of Physical Access Control

- * Confidentiality: Without physical control, organizations risk unauthorized physical access, potentially leading to data breaches.
- * Integrity: Physical tampering can compromise system configurations, software, or data integrity.
- * Availability: Physical tampering may result in downtime or service disruption.

Comparative Analysis of Options

- * B. Unable to track log on activity: Public cloud providers offer robust logging and monitoring tools, making this concern manageable with proper configurations.
- * C. Unable to run anti-virus scans: Cloud environments support anti-virus solutions and endpoint protections at various levels.
- * D. Unable to patch systems as needed: Public cloud providers facilitate regular patching through automated solutions and shared responsibility models.

EC-Council CISO References

- * Control and Oversight: EC-Council emphasizes understanding the shared responsibility model. While the cloud provider manages physical infrastructure, organizations are responsible for data and application security.
- * Mitigation Strategies: Implementing robust contractual agreements and auditing mechanisms ensures that the provider adheres to industry-standard physical security controls.

Conclusion

Among the listed concerns, the inability to control physical access to servers is the most pressing for public cloud computing due to the potential direct impact on the overall security posture. By prioritizing this, organizations align their risk management strategies with the EC-Council's frameworks for cloud security.

NEW QUESTION: 4

Which of the following provides the BEST ability to view potential financial results in relation to goal achievement?

- A. Savings-Delivery Analysis
- B. Cost-benefit analysis
- C. Business Impact Analysis
- D. Review of Investment

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies cost-benefit analysis (CBA) as the most effective method for evaluating potential financial results in relation to goal achievement. CBA directly compares the expected benefits of an initiative against its associated costs, enabling leadership to assess financial viability and return on investment.

CCISO guidance explains that CISOs must justify security investments in business terms, demonstrating how proposed controls reduce risk while supporting organizational objectives. Cost-benefit analysis supports executive decision-making by translating security initiatives into financial outcomes, which is critical for board-level discussions.

A Business Impact Analysis focuses on operational impact during disruptions, not financial outcomes of strategic goals. "Savings-Delivery Analysis" and "Review of Investment" are not formal CCISO analytical frameworks.

Therefore, per CCISO financial governance principles, cost-benefit analysis provides the best ability to evaluate financial results relative to goal achievement.

NEW QUESTION: 5

When reviewing a Solution as a Service (SaaS) provider's security health and posture, which key document should you review?

- A. SaaS provider's website certifications and representations (certs and reps)
- B. SOC-2 Report
- C. Metasploit Audit Report
- D. Statement from SaaS provider attesting their ability to secure your data

Answer: ([SHOW ANSWER](#))

* SOC-2 Report Overview:

* SOC-2 (System and Organization Controls) is a third-party audit report assessing a SaaS provider's controls related to security, availability, processing integrity, confidentiality, and privacy.

* It is specifically tailored for technology and SaaS companies, ensuring they meet critical trust service criteria.

* Relevance to SaaS Security Health:

* A SOC-2 report provides an objective assessment of the provider's security posture and internal controls.

* It demonstrates compliance with industry standards and instills confidence in the provider's ability to secure customer data.

* Why Not Other Options:

* A: Website certifications and representations may be useful but lack depth and validation.

* C: Metasploit audits focus on vulnerability assessments, not comprehensive security posture.

* D: Provider attestations are subjective and do not guarantee compliance with security frameworks.

Reference:

ThreatStack Compliance Guidance for SaaS Companies

Reference: <https://www.threatstack.com/blog/how-saas-companies-can-build-a-compliance-roadmap>

NEW QUESTION: 6

What are the three PRIMARY constraints of project management?

A. Scope, time, and cost

B. Time, quantity, and technology

C. Cost, quality, and people

D. Quality, deliverables, and cost

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation and standard project management principles referenced in the CCISO program, the three primary constraints-often called the project management triangle-are scope, time, and cost.

These constraints are interdependent: changes to one typically impact the others. CCISO materials emphasize that CISOs must understand these constraints to effectively manage security initiatives, communicate trade-offs to executives, and avoid project failure.

Quality and deliverables are outcomes influenced by the three primary constraints, not constraints themselves.

Therefore, Option A is correct.

NEW QUESTION: 7

An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program. What type of control has been effectively utilized?

A. Management Control

B. Technical Control

C. Training Control

D. Operational Control

Answer: (SHOW ANSWER)

Role of Security Awareness Training:

* Training controls enhance employees' ability to recognize and avoid sophisticated threats like spear phishing.

Effective Utilization:

* In this case, the employee's ability to avoid the attack demonstrates the success of the corporate information security awareness program.

Supporting Reference:

* CCISO materials emphasize the importance of training as a control to reduce human-related risks in security.

NEW QUESTION: 8

Which is the single MOST important factor for introducing digital evidence into a court of law?

- A. Uninterrupted chain of custody
- B. Comprehensive logs from all servers and network devices
- C. Fully trained network experts to analyze systems
- D. Expert security operations witnesses

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program identifies chain of custody as the most critical requirement for the admissibility of digital evidence in a court of law. Chain of custody documents who collected the evidence, how it was handled, where it was stored, and who accessed it, ensuring the evidence was not altered or tampered with.

CCISO materials emphasize that even the most compelling technical evidence can be ruled inadmissible if the chain of custody is broken or undocumented. Courts require proof that evidence integrity has been maintained from collection through presentation.

Logs, expert witnesses, and analysis tools (Options B-D) are valuable, but without an uninterrupted chain of custody, they cannot be legally relied upon. CCISO guidance aligns with forensic standards used in law enforcement and regulatory investigations.

Therefore, Option A is correct.

NEW QUESTION: 9

An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

- A. Data breach disclosure
- B. Consumer right disclosure
- C. Security incident disclosure
- D. Special circumstance disclosure

Answer: ([SHOW ANSWER](#))

Data Breach Notification Laws:

* Many jurisdictions mandate disclosure of data breaches to affected parties, including licensees and owners of personal information. Examples include GDPR, HIPAA, and state-level laws like the California Consumer Privacy Act (CCPA).

Purpose of Notification Laws:

* These laws aim to ensure transparency, protect consumer rights, and enable affected parties to take preventive actions.

Supporting Reference:

* The CCISO framework highlights the importance of compliance with breach notification laws to avoid legal penalties and maintain organizational trust.

NEW QUESTION: 10

Which of the following controls is MOST critical for protecting Artificial Intelligence (AI) systems?

- A. Public cloud
- B. Encrypted computer storage
- C. Hashed datasets
- D. Sanitized datasets

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge emphasizes that data integrity and data quality are foundational to the security of Artificial Intelligence systems. Among the listed options, sanitized datasets represent the most critical control for protecting AI systems. CCISO guidance highlights that AI systems are highly dependent on training and operational data, and any inclusion of sensitive, biased, poisoned, or malicious data can directly compromise outcomes, decisions, and trust.

Sanitization ensures that datasets are free from sensitive personal data, malicious injections, corrupted records, and unauthorized information. CCISO materials explicitly note that risks such as data poisoning, model manipulation, and unintended disclosure are unique and heightened in AI environments, making dataset sanitization a primary preventative control.

Encryption and hashing are important supporting controls, but CCISO guidance clarifies that they do not address model bias, poisoned training data, or unsafe inference behavior. Public cloud is not a control.

Therefore, sanitizing datasets before training and inference is the most critical control for AI security.

NEW QUESTION: 11

A security team member calls you to inform you that one of your databases might have been compromised, but there are no details available. As the security leader, what should you do?

- A. Tell her to initiate the incident response plan
- B. Tell her to provide updates as they become available
- C. Tell her to disconnect the servers connected to the database and call the help desk

D. Tell her to perform initial forensics and preserve system integrity

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to the EC-Council CCISO Body of Knowledge, the correct response to a suspected compromise- even without full details-is to initiate the incident response plan. CCISO guidance emphasizes that incident response plans are designed specifically for uncertain, evolving situations.

Initiating the plan does not imply panic or overreaction; instead, it activates predefined roles, communication paths, escalation criteria, and investigation procedures. CCISO materials stress that delaying activation until confirmation increases risk exposure and impact.

Performing forensics or disconnecting systems prematurely may destroy evidence or disrupt business unnecessarily. Waiting for updates without action contradicts CCISO guidance on proactive response.

Thus, initiating the incident response plan is the most appropriate leadership action.

NEW QUESTION: 12

Which of the following has the GREATEST impact on the implementation of an information security governance model?

- A.** Organizational budget
- B.** Distance between physical locations
- C.** Number of employees
- D.** Complexity of organizational structure

Answer: ([SHOW ANSWER](#))

Impact of Organizational Complexity:

* The complexity of an organization's structure directly affects how governance models are implemented and managed. Complex structures often require more tailored and decentralized governance approaches.

Governance Challenges in Complex Structures:

* CCISO materials highlight that factors such as interdepartmental coordination, diverse regulatory requirements, and multiple stakeholders can complicate governance implementation.

Supporting Reference:

* CCISO emphasizes understanding organizational intricacies as a key factor for tailoring governance models to ensure effective control and oversight mechanisms.

NEW QUESTION: 13

Which of the following is MOST effective when mitigating social engineering risks?

- A.** Threat and Vulnerability Management Programs
- B.** Phishing tests
- C.** Anti-malware tools
- D.** Security awareness programs

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, the most effective control for mitigating social engineering risk is a security awareness program. CCISO materials emphasize that social engineering exploits human behavior, not technical vulnerabilities, making people the primary control surface.

Anti-malware tools (Option C) protect systems, not decision-making. Threat and vulnerability management programs (Option A) address technical weaknesses. Phishing tests (Option B) are valuable measurement tools, but they are components of a broader awareness program, not standalone mitigations.

CCISO guidance highlights that sustained, role-based security awareness programs reduce successful social engineering attacks by educating users on threat recognition, reporting procedures, and expected behaviors.

These programs are foundational to insider threat reduction and are reinforced through continuous training and executive sponsorship.

Thus, Option D is correct.

NEW QUESTION: 14

A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority?

- A.** Have internal audit conduct another audit to see what has changed.
- B.** Contract with an external audit company to conduct an unbiased audit
- C.** Review the recommendations and follow up to see if audit implemented the changes
- D.** Meet with audit team to determine a timeline for corrections

Answer: ([SHOW ANSWER](#))

Initial Assessment for a New CISO:

- * Upon starting a new role, the CISO's first task is to understand the current security posture by evaluating existing reports, audits, and documentation.
- * The two-year-old audit report provides a starting point to identify gaps and determine if previous recommendations were implemented.

Why Following Up on Audit Recommendations is the First Priority:

- * Ensures critical findings from the previous audit have been addressed, which could mitigate potential risks.
- * Provides insight into the organization's ability to act on audit findings and close gaps effectively.
- * Highlights areas where improvements are still needed.

Why Other Options Are Incorrect:

- * A. Conduct another internal audit: Premature; following up on the existing audit is more immediate and actionable.
- * B. Contract with an external audit company: Adds cost and delays addressing known issues.

* D. Meet with the audit team for corrections timeline: Important but secondary to verifying the status of previous recommendations.

References:

EC-Council emphasizes the importance of evaluating and following up on past audit findings as a foundational step for a CISO in assessing the current security environment.

NEW QUESTION: 15

Which of the following BEST describes revenue?

- A.** The economic benefit derived by operating a business
- B.** The sum value of all assets and cash flow into the business
- C.** Non-operating financial liabilities minus expenses
- D.** The future profit-making potential of an organization

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge defines revenue as the economic benefit generated from normal business operations, typically through the sale of goods or services. CCISO finance and strategy modules emphasize that revenue represents income earned before expenses, taxes, and liabilities are deducted.

Option A correctly reflects this definition. Option B incorrectly combines assets and cash flow, which are balance-sheet concepts rather than revenue. Option C describes a financial calculation unrelated to revenue, while option D refers to organizational valuation or goodwill, not revenue. CCISO materials stress that CISOs must understand revenue because security decisions can directly impact revenue generation through system availability, customer trust, and regulatory compliance. Therefore, understanding revenue as operational income is essential for business-aligned security leadership.

NEW QUESTION: 16

Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

- A.** The Net Present Value (NPV) of the project is negative
- B.** The Return on Investment (ROI) is less than 10 months
- C.** The Return on Investment (ROI) is longer than 10 months
- D.** The Net Present Value (NPV) of the project is positive

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies negative Net Present Value (NPV) as the most common reason executives reject proposed projects. NPV measures whether the discounted future benefits exceed the initial and ongoing costs of an investment.

CCISO financial governance modules emphasize that boards prioritize investments that create or preserve value. A negative NPV indicates that a project destroys value, even if it has security benefits. While ROI timing may influence prioritization, it rarely results in outright rejection if NPV is positive.

CCISO materials stress that CISOs must frame security investments in financial terms, demonstrating long-term value creation or loss avoidance. A positive NPV indicates value, while a negative NPV signals financial inefficiency.

Therefore, a negative NPV is the most probable reason for rejection.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam! ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examd Discuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

- A. Security certification
- B. Security system analysis
- C. Security accreditation
- D. Alignment with business practices and goals.

Answer: (SHOW ANSWER)

Definition of Security Accreditation

Security accreditation is the formal approval by management of the security certification process. It documents the identified risks, their mitigations, and establishes the acceptability of residual risks for an IT system.

Steps in the Process

- * Review findings from the security certification process.
- * Assess residual risks and proposed mitigations.
- * Obtain formal approval from authorized personnel.

Comparison of Options

- * A. Security certification: Precedes accreditation and focuses on technical validation.
- * B. Security system analysis: Broad assessment, not specific to the certification-accreditation lifecycle.
- * D. Alignment with business practices and goals: Pertains to overall strategic alignment, not risk acceptance.

EC-Council References

* This process ensures management involvement and accountability, which aligns with CISO responsibilities under risk management frameworks taught by EC-Council.

NEW QUESTION: 18

Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed. What can be done to ensure that security is addressed cost effectively?

- A.** User awareness training for all employees
- B.** Installation of new firewalls and intrusion detection systems
- C.** Launch an internal awareness campaign
- D.** Integrate security requirements into project inception

Answer: ([SHOW ANSWER](#))

* By integrating security requirements from the beginning of a project, security is built-in rather than treated as an afterthought.

* This approach reduces costs and ensures compliance with security objectives throughout the project lifecycle.

Why Other Options Are Incorrect:

* A. User awareness training: Important but does not address the systemic issue of integrating security into project planning.

* B. Installation of new firewalls: A technical solution that addresses only part of the broader need for integrated security.

* C. Launch an awareness campaign: Awareness is helpful but does not ensure cost-effective security implementation.

EC-Council CISO Reference:

The program stresses security-by-design principles to minimize costs and maximize effectiveness.

NEW QUESTION: 19

Which of the following are necessary to formulate responses to external audit findings?

- A.** Internal Audit, Management, and Technical Staff
- B.** Internal Audit, Budget Authority, Management
- C.** Technical Staff, Budget Authority, Management
- D.** Technical Staff, Internal Audit, Budget Authority

Answer: ([SHOW ANSWER](#))

Formulating Responses to Audit Findings:

* Internal audit provides oversight and ensures the findings are addressed effectively.

* Management ensures alignment with organizational objectives and secures necessary resources.

* Technical staff implements the required changes and provides technical feasibility insights.

Why This is Correct:

* The combination of these groups ensures a comprehensive response, addressing technical and organizational aspects of the findings.

Why Other Options Are Incorrect:

* B, C, D: Exclude critical stakeholders (e.g., internal audit or technical staff), limiting effectiveness.

References:

EC-Council emphasizes collaboration among audit teams, management, and technical staff to formulate effective responses to audit findings.

NEW QUESTION: 20

A missing/ineffective security control is identified. Which of the following should be the NEXT step?

- A. Perform an audit to measure the control formally
- B. Escalate the issue to the IT organization
- C. Perform a risk assessment to measure risk
- D. Establish Key Risk Indicators

Answer: ([SHOW ANSWER](#))

Next Step After Identifying a Missing Control:

* A risk assessment determines the potential impact and likelihood of the risk posed by the missing or ineffective control.

Purpose of the Assessment:

* This step quantifies the risk to prioritize and inform decision-making regarding mitigation strategies.

Supporting Reference:

* CCISO emphasizes risk assessment as a foundational step in addressing control gaps, ensuring risks are evaluated systematically.

NEW QUESTION: 21

The new CISO was informed of all the Information Security projects that the organization has in progress.

Two projects are over a year behind schedule and over budget. Using best business practices for project management you determine that the project correctly aligns with the company goals.

Which of the following needs to be performed NEXT?

- A. Verify the scope of the project
- B. Verify the regulatory requirements
- C. Verify technical resources
- D. Verify capacity constraints

Answer: ([SHOW ANSWER](#))

Next Steps in Project Management

* Verifying the project scope ensures alignment with organizational goals and confirms whether the project objectives are well-defined and achievable within the current parameters.

* Adjustments to scope may be necessary to address delays and budget overruns effectively.

Why Not Other Options?

- * B. Verify regulatory requirements: Important, but the scenario emphasizes project performance, not compliance.
- * C. Verify technical resources: Relevant, but scope validation is prioritized to identify underlying issues.
- * D. Verify capacity constraints: Pertains to resource management but follows scope verification.

EC-Council References

- * Highlights scope management as a foundational element in effective project management.

NEW QUESTION: 22

What is MOST critical when managing the critical path of a project?

- A. Knowing the minimum requirements for project acceptance
- B. Knowing milestones and timelines of deliverables
- C. Knowing the stakeholders and their peers
- D. Knowing the vulnerabilities of milestones

Answer: (SHOW ANSWER)

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to the EC-Council CCISO Body of Knowledge, the most critical aspect of managing a project's critical path is understanding the milestones and timelines of deliverables. The critical path represents the sequence of tasks that determine the minimum project duration.

CCISO materials explain that delays in critical path tasks directly delay the entire project.

Therefore, accurate visibility into dependencies, schedules, and milestone completion is essential for risk management, resource allocation, and executive reporting.

Stakeholder awareness and acceptance criteria are important, but they do not define the critical path.

Vulnerabilities relate to risk, not scheduling.

Thus, knowing milestones and timelines is the most critical factor when managing the critical path.

NEW QUESTION: 23

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

- A. When there is a need to develop a more unified incident response capability.
- B. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.
- C. When there is a variety of technologies deployed in the infrastructure.
- D. When it results in an overall lower cost of operating the security program.

Answer: (SHOW ANSWER)

When Decentralized Policies Are Beneficial:

- * In organizations with varied business units, a one-size-fits-all approach may not be effective.

Decentralized policies allow tailoring to specific risks, operations, and regulatory demands of individual units.

Advantages of Decentralization:

- * Greater flexibility to meet unit-specific needs.
- * Improved compliance with diverse regulatory environments.

Why Other Options Are Incorrect:

- * A. Unified Incident Response: Requires centralized, not decentralized, coordination.
- * C. Technology Variety: Centralized policies ensure consistency in handling diverse technologies.
- * D. Cost Efficiency: Decentralization may lead to higher costs due to duplication of efforts.

References:

EC-Council supports decentralization in cases where organizational diversity necessitates tailored policies and procedures for effective risk management.

NEW QUESTION: 24

Which of the following is the MOST important to share with an Information Security Steering Committee:

- A.** Include a mix of members from different departments and staff levels
- B.** Review audit and compliance reports
- C.** Ensure that security policies and procedures have been vetted and approved
- D.** Be briefed about new trends and products at each meeting by a vendor

Answer: (SHOW ANSWER)

- * Purpose of the Information Security Steering Committee
- * The Information Security Steering Committee (ISSC) oversees the organization's information security program, ensuring alignment with strategic goals and regulatory requirements. Sharing critical information, such as audit and compliance reports, enables informed decision-making and prioritization of security initiatives.
- * Importance of Audit and Compliance Reports
- * Audit Reports: These highlight vulnerabilities, non-compliance areas, and operational inefficiencies. Reviewing audit reports helps the ISSC address gaps proactively.
- * Compliance Reports: These ensure the organization meets regulatory and legal requirements, reducing the risk of fines, legal action, and reputational damage.
- * Sharing these reports ensures the committee is updated on the organization's current security posture and areas needing improvement.
- * Explanation of Other Options
- * A. Include a mix of members from different departments and staff levels: While having diverse members is beneficial for representation and perspective, it is not information to be "shared" with the committee.
- * C. Ensure that security policies and procedures have been vetted and approved: This is an operational requirement rather than the primary focus of information sharing during committee meetings.

* D. Be briefed about new trends and products at each meeting by a vendor: Briefings from vendors may be useful occasionally but are not as critical as reviewing audit and compliance reports for ensuring the organization's security posture.

* EC-Council CISO Guidance

* The EC-Council CISO framework emphasizes the importance of governance, where oversight bodies like the ISSC are provided with actionable insights derived from audits and compliance evaluations. This allows the committee to make strategic decisions and enforce accountability.

NEW QUESTION: 25

What is the primary reason for performing a return on investment analysis?

- A. To decide between multiple vendors
- B. To decide if the solution costs less than the risk it is mitigating
- C. To determine the current present value of a project
- D. To determine the annual rate of loss

Answer: ([SHOW ANSWER](#))

The primary purpose of a return on investment (ROI) analysis in cybersecurity is to determine if the cost of implementing a solution is justified by the risk reduction or benefits it provides.

* Purpose of ROI Analysis:

* Evaluates the financial impact of a proposed solution in mitigating identified risks.

* Helps determine whether the cost is outweighed by the value gained (risk reduction or operational efficiency).

* Key Considerations:

* Includes both tangible benefits (e.g., cost savings) and intangible benefits (e.g., reputation protection).

* Guides decision-making between implementing or forgoing a solution.

* Other Options:

* Vendor Selection: ROI is not limited to vendor comparison.

* Present Value Calculation: ROI is broader, encompassing benefits over costs.

* Annual Loss Expectancy (ALE): A related metric but not the primary purpose of ROI.

* Risk-Based Decision Making: EC-Council emphasizes aligning investments with risk mitigation goals.

* Economic Evaluation in Security Projects: ROI analysis supports strategic resource allocation.

NEW QUESTION: 26

When you develop your audit remediation plan what is the MOST important criteria?

- A. To remediate half of the findings before the next audit.
- B. To remediate all of the findings before the next audit.
- C. To validate that the cost of the remediation is less than the risk of the finding.
- D. To validate the remediation process with the auditor.

Answer: ([SHOW ANSWER](#))

Importance of Cost-Risk Analysis

* The EC-Council CISO framework emphasizes the principle of risk-based decision-making in all cybersecurity processes, including audit remediation. Addressing audit findings requires organizations to evaluate the potential risks associated with each finding and prioritize remediation efforts based on their cost-effectiveness.

* Ensuring that the cost of remediation is proportional to the risk mitigated avoids unnecessary expenditures while addressing critical vulnerabilities.

Comparison with Other Options

* A. To remediate half of the findings before the next audit: This approach lacks a strategic foundation.

Arbitrarily remediating half of the findings does not align with a risk-based strategy, leading to potential neglect of high-priority issues.

* B. To remediate all of the findings before the next audit: While remediating all findings is ideal, it is often impractical due to resource constraints. A prioritized, risk-based approach ensures critical vulnerabilities are addressed first, maximizing the impact of remediation efforts.

* D. To validate the remediation process with the auditor: Although validation with the auditor is a good practice, it is a secondary step. The primary focus must be on ensuring that remediation efforts align with risk mitigation objectives and resource efficiency.

EC-Council CISO Guidance on Audit Remediation Plans

* The framework highlights these critical steps:

* Risk Assessment: Analyze the severity and potential impact of findings.

* Cost-Benefit Analysis: Determine if the remediation cost is justified by the reduction in risk exposure.

* Prioritization: Address high-risk findings first, ensuring critical vulnerabilities are mitigated promptly.

* Alignment with Organizational Goals: Ensure remediation efforts support broader business and security objectives.

Balancing Compliance and Practicality

* An effective audit remediation plan balances compliance requirements with practical considerations.

Overcommitting resources to less impactful findings can divert attention from critical risks.

* Validating the cost-risk ratio ensures that resources are utilized effectively, enabling sustainable compliance and operational resilience.

Conclusion

* The most important criterion when developing an audit remediation plan is to validate that the cost of the remediation is less than the risk of the finding. This approach ensures that the organization prioritizes its efforts effectively, aligns with risk management principles, and maximizes resource utilization.

NEW QUESTION: 27

With respect to the audit management process, management response serves what function?

A. placing underperforming units on notice for failing to meet standards

- B. determining whether or not resources will be allocated to remediate a finding
- C. adding controls to ensure that proper oversight is achieved by management
- D. revealing the "root cause" of the process failure and mitigating for all internal and external units

Answer: ([SHOW ANSWER](#))

Function of Management Response in Audits:

* The management response evaluates audit findings and decides on resource allocation for addressing identified issues.

Purpose:

* This step ensures that management's priorities align with the organization's risk management and operational goals.

Supporting Reference:

* CCISO materials emphasize management's role in assessing and addressing audit findings to improve organizational processes.

NEW QUESTION: 28

Controls that were implemented to correct prior audit findings are insufficient. Before adjusting controls, what original document should be reviewed?

- A. Business recovery plan
- B. Business Impact Analysis
- C. Security process catalogue
- D. Annual report to shareholders

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to CCISO guidance, the security process catalogue should be reviewed before adjusting controls.

CCISO materials explain that controls are derived from documented processes; ineffective controls often indicate flawed or incomplete processes.

Reviewing the process catalogue ensures controls align with intended workflows and responsibilities before modification. Other documents do not define control-process relationships.

NEW QUESTION: 29

Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

- A. Network based security preventative controls
- B. Software segmentation controls
- C. Network based security detective controls
- D. User segmentation controls

Answer: ([SHOW ANSWER](#))

Definition and Role

* Network-based security preventative controls are measures designed to prevent unauthorized access, attacks, or breaches. Examples include:

- * Access Control Lists (ACLs): Define rules for network traffic.
- * Firewalls: Block unauthorized traffic based on predefined rules.
- * Intrusion Prevention Systems (IPS): Actively block identified threats.

Comparison of Options

- * B. Software segmentation controls: Related to application security, not network-level security.
- * C. Network-based security detective controls: These include tools like IDS, which detect but do not prevent attacks.
- * D. User segmentation controls: Focus on user-based access restrictions, not network controls.

EC-Council References

- * Highlighted in network security strategies as critical tools for perimeter defense and attack prevention.

NEW QUESTION: 30

What should an auditor do after discovering that a security analyst is working a late-night shift every week as the senior server administrator?

- A. Inform the security officer of the need for an exception
- B. Inform senior management of the risk
- C. Immediately review the system logs of all servers
- D. Ensure additional monitoring is applied to the security analyst

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to the EC-Council CCISO Body of Knowledge, auditors are responsible for identifying and reporting governance, risk, and control weaknesses, not implementing operational fixes. The scenario described represents a segregation of duties (SoD) violation, where a security analyst is also performing senior server administrator duties on a recurring basis.

CCISO documentation emphasizes that segregation of duties is a foundational internal control designed to prevent fraud, abuse, and unauthorized activity. When one individual holds both monitoring and administrative authority, the organization faces an elevated risk of undetected malicious or accidental actions.

This is considered a material risk requiring executive awareness.

The CCISO framework states that once such a risk is identified, the auditor's proper course of action is to formally report the risk to senior management. Executive leadership is accountable for risk acceptance, remediation prioritization, and allocation of resources. Auditors must remain independent and should not direct operational activities such as log reviews or monitoring changes.

Options A, C, and D represent management or operational actions, which fall outside the auditor's role.

CCISO guidance clearly distinguishes between risk identification and risk treatment responsibilities.

Therefore, per CCISO principles, the auditor should inform senior management of the risk, making option B the correct answer.

NEW QUESTION: 31

A recent audit has identified control exceptions and recommends implementing technology and processes to remediate the finding. Which of the following is the MOST likely reason for the organization to reject the recommendation?

- A. The organization has focused only on regulatory issues
- B. The auditors have not followed proper auditing processes
- C. The business agrees with the finding
- D. The situation is within the risk tolerance of the organization

Answer: (SHOW ANSWER)

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge emphasizes that audit findings do not automatically require remediation. One of the core principles of governance is risk acceptance, where management formally decides that a risk falls within the organization's defined risk tolerance. CCISO documentation explains that senior leadership is responsible for determining whether identified risks should be mitigated, transferred, avoided, or accepted. If the cost of remediation outweighs the potential impact, or if the risk aligns with strategic objectives, management may legitimately choose to accept the risk and reject the recommendation.

Rejecting a recommendation does not imply auditors were incorrect or that the organization ignores security.

Instead, it reflects risk-based decision-making, a foundational CCISO concept. Agreement with the finding does not require remediation, and regulatory focus does not automatically negate risk acceptance.

Therefore, the most likely and CCISO-validated reason for rejecting the recommendation is that the situation is within the organization's risk tolerance.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!

ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

In order to improve situational awareness, there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which of the following tools represents the BEST choice to achieve this awareness?

- A.** Security Information and Event Management (SIEM), Intrusion Prevention Systems (IPS), routers, and server alerts
- B.** Intrusion Detection Systems (IDS), firewalls, switches, and system compliance tools
- C.** Virtualized servers, routers, firewalls, and system logs
- D.** Security Information and Event Management (SIEM), Intrusion Detection Systems (IDS), firewalls, and Vulnerability Management Systems (VMS)

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, the most effective way to achieve enterprise-wide situational awareness is through integrated security monitoring, centered on SIEM technology.

SIEM platforms aggregate and correlate events from IDS, firewalls, vulnerability management systems, and other security controls, providing real-time visibility, context, and analytics. CCISO materials emphasize correlation and centralization as essential for executive-level awareness.

Options A, B, and C lack comprehensive correlation or vulnerability context. Only Option D combines detection, prevention, and vulnerability intelligence into a unified view.

Therefore, Option D is correct.

NEW QUESTION: 33

When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?

- A.** This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
- B.** Contracting rules typically require you to have conversations with two or more groups
- C.** Discussing decisions with a very large group of people always provides a better outcome
- D.** It helps to avoid regulatory or internal compliance issues

Answer: ([SHOW ANSWER](#))

Collaboration among stakeholders such as lawyers, IT security professionals, privacy experts, and engineers ensures that new products and services meet legal, regulatory, and internal compliance requirements. This multi-disciplinary approach reduces the risk of breaches, fines, or operational inefficiencies. Options A, B, and C are not valid or comprehensive reasons for engaging these groups during procurement processes.

Reference: <https://www.eccouncil.org/wp-content/uploads/2016/07/NICE-2.0-and-EC-Council-Cert-Mapping.pdf>

pdf

Reference: <https://www.eccouncil.org/wp-content/uploads/2016/07/NICE-2.0-and-EC-Council-Cert-Mapping.pdf>

pdf

NEW QUESTION: 34

Credit card information, medical data, and government records are all examples of:

- A. Confidential/Protected Information
- B. Bodily Information
- C. Territorial Information
- D. Communications Information

Answer: ([SHOW ANSWER](#))

Definition of Confidential/Protected Information: Confidential or protected information encompasses any data that must be safeguarded from unauthorized access or disclosure to ensure its confidentiality, integrity, and availability. This category includes sensitive personal, financial, medical, and proprietary information.

Examples of Confidential/Protected Information:

- * Credit Card Information: Financial data that requires compliance with PCI-DSS standards for secure handling and processing.
- * Medical Data: Protected under regulations such as HIPAA in the U.S., ensuring privacy and security of patient health information.
- * Government Records: Often classified or protected under laws and regulations to maintain national security and ensure the privacy of sensitive governmental operations.

Key References:

- * The EC-Council Certified CISO (CCISO) framework specifically identifies the handling and protection of such data as a core responsibility under the domain of Information Security Management.
- * Per EC-Council CCISO material, such data forms the backbone of risk assessment and compliance mandates in most regulatory frameworks.

Connection to Cybersecurity Best Practices: As per the CCISO guidelines, proper classification and protection of this type of information are paramount. This involves:

- * Establishing security policies.
- * Implementing technical controls such as encryption and access control.
- * Training employees to recognize and handle sensitive data appropriately.

NEW QUESTION: 35

Which of the following defines the boundaries and scope of a risk assessment?

- A. The risk assessment schedule
- B. The risk assessment framework
- C. The risk assessment charter
- D. The assessment context

Answer: ([SHOW ANSWER](#))

* Assessment Context Definition:

- * The assessment context defines the boundaries and scope of a risk assessment by identifying what will be included or excluded, such as assets, processes, or business units.

- * Components of Context:
- * Clearly specifies geographical, organizational, and operational scope.
- * Determines external and internal factors influencing the risk assessment.
- * Importance:
- * Provides clarity on what needs to be assessed and ensures stakeholders align their expectations.

References:

- * EC-Council CISO Handbook on Risk Management Frameworks.
- * CFocus Software Guidance on Risk Assessment Boundaries.

Reference: <https://cfocussoftware.com/risk-management-framework/know-your-boundary/>

NEW QUESTION: 36

A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen and the database server was disconnected. Who must be informed of this incident?

- A. Internal audit
- B. The data owner
- C. All executive staff
- D. Government regulators

Answer: (SHOW ANSWER)

Role of the Data Owner:

The data owner is accountable for the confidentiality, integrity, and availability of the data. They must be informed immediately in case of a security breach to make critical decisions about remediation and further protection.

Why This Answer Is Correct:

- * The data owner determines the business impact of the breach.
- * They decide on necessary actions, such as notifying stakeholders or regulators.

Why Other Options Are Incorrect:

- * A. Internal Audit: Ensures compliance but is not involved in operational incident handling.
- * C. All Executive Staff: Only informed if the incident's scope affects business-critical functions.
- * D. Government Regulators: Informed only when required by law or policy after initial assessments.

References:

EC-Council emphasizes the responsibility of data owners in managing incidents affecting their assets and collaborating with response teams.

NEW QUESTION: 37

In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

- A. Internal Audit
- B. Database Administration

C. Information Security

D. Compliance

Answer: ([SHOW ANSWER](#))

Role of Information Security:

* The information security team is typically responsible for monitoring intrusion detection system (IDS) logs to identify and respond to threats.

Operational Responsibilities:

* Regular log reviews are a key task in maintaining network security and ensuring proactive threat management.

Supporting Reference:

* CCISO training describes log analysis and monitoring as core responsibilities of information security operations.

NEW QUESTION: 38

What oversight should the information security team have in the change management process for application security?

A. Information security should be aware of all application changes and work with developers before changes are deployed in production

B. Information security should be aware of any significant application security changes and work with developer to test for vulnerabilities before changes are deployed in production

C. Development team should tell the information security team about any application security flaws

D. Information security should be informed of changes to applications only

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

During an initial investigation, the Incident Response Team suspects criminal activity but cannot initially prove or disprove illegal actions. What is the MOST critical action they should take?

A. Preservation of evidence

B. Constant communication of status to executives

C. Eradication of malware and system restoration

D. Determination of the attack source

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge clearly identifies preservation of evidence as the most critical action when criminal activity is suspected during an incident investigation. CCISO incident response guidance emphasizes that when illegality is possible-even if not yet confirmed-the organization must assume that evidence may be required for legal, regulatory, or law enforcement proceedings.

Preserving evidence ensures the integrity, admissibility, and credibility of digital artifacts such as logs, memory captures, disk images, and network traffic. CCISO materials stress that premature eradication, system restoration, or investigative actions can unintentionally destroy or alter evidence, undermining legal action and exposing the organization to liability.

While executive communication is important, CCISO guidance clearly prioritizes chain of custody and forensic soundness over status reporting. Determining the attack source and eradicating malware are subsequent steps that should occur only after evidence is preserved.

The CCISO framework also highlights that CISOs must coordinate with legal counsel when criminal activity is suspected, and this coordination depends on preserved evidence. Therefore, preservation of evidence is the foundational action that enables all other response activities.

In summary, CCISO doctrine confirms that preserving evidence is the most critical action during early incident response when criminal activity is suspected.

NEW QUESTION: 40

After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

- A. Risk Tolerance
- B. Qualitative risk analysis
- C. Risk Appetite
- D. Quantitative risk analysis

Answer: ([SHOW ANSWER](#))

Quantitative Risk Analysis:

- * This method involves assigning numerical values to risks, typically in monetary terms, to assess potential impacts.
- * The example provided (1.2 Million USD) is a direct application of quantitative analysis.

Purpose of Quantitative Analysis:

- * Helps in prioritizing risks based on their financial implications and aids in decision-making for risk mitigation strategies.

Supporting Reference:

- * The CCISO framework explains quantitative risk analysis as part of enterprise risk assessment to quantify and prioritize risks effectively.

NEW QUESTION: 41

Which regulation or policy governs protection of personally identifiable user data gathered during a cyber investigation?

- A. ITIL
- B. Privacy Act
- C. Sarbanes Oxley
- D. PCI-DSS

Answer: ([SHOW ANSWER](#))

The Privacy Act governs the protection of personally identifiable information (PII) collected during investigations. It mandates safeguards to ensure PII is not misused or improperly disclosed. Regulations like Sarbanes-Oxley (C) focus on financial disclosures, PCI-DSS (D) on payment card data security, and ITIL (A) on IT service management, making them unrelated to user data protection in cyber investigations.

NEW QUESTION: 42

In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

- A.** Distance learning/Web seminars
- B.** Formal Class
- C.** One-One Training
- D.** Self -Study (noncomputerized)

Answer: ([SHOW ANSWER](#))

- * Distance learning and web seminars are cost-effective training methods as they eliminate travel, venue, and material costs while allowing scalability to train multiple individuals simultaneously.
- * These methods also offer flexibility for learners, reducing productivity loss during training.

Why Other Options Are Less Cost-Effective:

- * B. Formal class: Involves significant costs for instructors, venues, and travel.
- * C. One-on-one training: Highly personalized but not cost-effective due to time and resource demands.
- * D. Self-study (noncomputerized): May have minimal costs but lacks scalability and standardization.

EC-Council CISO Reference:

Cost-effective training solutions are emphasized as critical for maintaining skills while managing organizational budgets effectively.

NEW QUESTION: 43

As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?

- A.** Dual Control
- B.** Separation of Duties
- C.** Split Knowledge
- D.** Least Privilege

Answer: ([SHOW ANSWER](#))

Split knowledge ensures that no single individual can independently generate or reconstruct an encryption key. This principle divides knowledge of the key among multiple individuals, requiring their collaboration for key generation or usage. While dual control involves multiple individuals acting together, split knowledge specifically ensures that individual actions alone cannot

compromise key integrity. Separation of duties and least privilege focus on broader security principles rather than encryption-specific safeguards.

Reference: <https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management>

NEW QUESTION: 44

Which level of data destruction applies logical techniques to sanitize data in all user-addressable storage locations?

- A. Purge
- B. Clear
- C. Mangle
- D. Destroy

Answer: (SHOW ANSWER)

Purge involves applying logical techniques to sanitize data in all user-addressable storage locations, ensuring the data is unrecoverable without using laboratory techniques. This is a higher level of data destruction than clearing (logical removal allowing some recovery) and distinct from physical destruction (destroying storage media). Mangle is not a recognized data destruction standard.

Reference: <https://it.brown.edu/computing-policies/electronic-equipment-disposition-policy/data-removal-recommendations>

NEW QUESTION: 45

Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

- A. Senior Executives
- B. Office of the Auditor
- C. Office of the General Counsel
- D. All employees and users

Answer: (SHOW ANSWER)

Primary Responsibility of Senior Executives:

- * Under the InfoSec governance framework, senior executives are tasked with providing oversight of the organization's comprehensive information security program. They ensure alignment with business goals and risk management strategies.

Role in Governance:

- * Senior executives set the tone at the top, allocate resources, and oversee the implementation of security policies and frameworks.

Supporting Reference:

- * CCISO materials identify senior executives as key stakeholders in InfoSec governance, responsible for strategic oversight.

NEW QUESTION: 46

Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.

Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

- A. National Institute of Standards and Technology (NIST) Special Publication 800-53
- B. Payment Card Industry Digital Security Standard (PCI DSS)
- C. International Organization for Standardization - ISO 27001/2
- D. British Standard 7799 (BS7799)

Answer: (SHOW ANSWER)

The ISO 27001/2 framework is industry- and sector-neutral, making it ideal for organizations without an established security framework.

* Framework Overview:

* ISO 27001/2: Globally recognized for establishing an Information Security Management System (ISMS).

* Flexible and adaptable across industries, ensuring relevance to varied organizational needs.

* Why Other Frameworks Are Less Suitable:

* NIST SP 800-53: Comprehensive but U.S.-centric, primarily focused on federal systems.

* PCI DSS: Industry-specific, tailored for payment card security.

* BS 7799: Precursor to ISO 27001, largely superseded.

* Benefits of ISO 27001/2:

* Offers a structured approach to managing sensitive information.

* Provides globally accepted best practices for implementation.

* Control Frameworks: Recommends ISO 27001/2 for organizations seeking an adaptable, globally accepted approach.

* Strategic Security Planning: Highlights the benefits of sector-neutral frameworks for establishing comprehensive security programs.

Scenario2

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!

ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 47

Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture.

What would be the BEST choice of security metrics to present to the BOD?

- A. All vulnerabilities found on servers and desktops
- B. Only critical and high vulnerabilities on servers and desktops
- C. Only critical and high vulnerabilities that impact important production servers
- D. All vulnerabilities that impact important production servers

Answer: ([SHOW ANSWER](#))

Focus on Relevant Metrics:

* The Board of Directors (BOD) requires concise, impactful information that demonstrates the organization's security posture. Metrics should highlight risks that directly affect critical business operations.

Presentation Strategy:

* Highlighting only critical and high vulnerabilities on production servers ensures the BOD understands the urgency and importance of these vulnerabilities without overwhelming them with irrelevant details.

Supporting Reference:

* CCISO materials emphasize presenting risk-based metrics that align with organizational priorities to effectively communicate with executive leadership.

NEW QUESTION: 48

At which point should the identity access management team be notified of the termination of an employee?

- A. At the end of the day once the employee is off site
- B. During the monthly review cycle
- C. Immediately so the employee account(s) can be disabled
- D. Before an audit

Answer: ([SHOW ANSWER](#))

Importance of Immediate Notification:

* Promptly notifying the identity access management team ensures that accounts are disabled to prevent unauthorized access after termination.

Best Practices for Access Management:

* Delayed action can result in security vulnerabilities, including misuse of active credentials.

Supporting Reference:

* CCISO materials stress the importance of timely account management to mitigate insider threats and maintain security integrity.

NEW QUESTION: 49

What is the MAIN reason for conflicts between Information Technology and Information Security programs?

- A.** Technology governance defines technology policies and standards while security governance does not.
- B.** Security governance defines technology best practices and Information Technology governance does not.
- C.** Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
- D.** The effective implementation of security controls can be viewed as an inhibitor to rapid Information Technology implementations.

Answer: (SHOW ANSWER)

Conflict Between IT and Security Programs:

- * IT teams often prioritize rapid deployment and operational efficiency.
- * Security teams focus on safeguarding assets, which can introduce delays and additional controls.

Main Cause of Conflict:

- * Security controls like access restrictions and rigorous testing may be seen as obstacles to IT's speed- oriented goals.

Why Other Options Are Incorrect:

- * A, B, C: While governance focuses differ, the primary issue is the perceived impact of security on IT speed.

References:

EC-Council highlights the need for collaboration between IT and security to balance operational agility with risk mitigation.

NEW QUESTION: 50

A Security Operations Manager is finding it difficult to maintain adequate staff levels to monitor security operations during off-hours. To reduce the impact of staff shortages and increase coverage during off-hours, the SecOps manager is considering outsourcing off-hour coverage.

What Security Operations Center (SOC) model does this BEST describe?

- A.** Virtual SOC
- B.** In-house SOC
- C.** Security Network Operations Center (SNOC)
- D.** Hybrid SOC

Answer: (SHOW ANSWER)

* Hybrid SOC Model Defined:

- * Combines in-house and outsourced services to extend coverage, particularly during off-hours.
- * Provides flexibility to handle staffing shortages while ensuring 24/7 monitoring.

* Why Not Other Options:

- * A: Virtual SOC's are fully outsourced, not hybrid.
- * B: In-house SOC's require full internal staffing, making them unsuitable during shortages.
- * C: SNOC's integrate network and security operations but are unrelated to outsourcing.

References:

* TechTarget on SOC Models and Hybrid SOC Benefits

Reference: <https://www.techtarget.com/searchsecurity/tip/Benefits-of-virtual-SOCs-Enterprise-run-vs-fully-managed>

NEW QUESTION: 51

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.

Which of the following frameworks and standards will BEST fit the organization as a baseline for their security program?

- A. NIST and Privacy Regulations
- B. ISO 27000 and Payment Card Industry Data Security Standards
- C. NIST and data breach notification laws
- D. ISO 27000 and Human resources best practices

Answer: B (LEAVE A REPLY)

Best Fit for a Security Baseline

* ISO 27000 provides a robust framework for building an information security management system (ISMS), applicable to organizations of any size and industry.

* PCI DSS is specifically tailored for organizations handling credit card transactions, ensuring secure payment processing and compliance.

Why Not Other Options?

- * A. NIST and Privacy Regulations: NIST provides detailed controls but lacks a global focus and industry-specific guidelines like PCI DSS.
- * C. NIST and Data Breach Notification Laws: Data breach laws are reactive, not foundational for a security baseline.
- * D. ISO 27000 and Human Resources Best Practices: HR practices are not a direct fit for a security program baseline.

EC-Council References

* EC-Council emphasizes ISO 27000 for ISMS and PCI DSS for payment-related security in retail environments.

NEW QUESTION: 52

Which of the following is a countermeasure to prevent unauthorized database access from Web applications?

- A. Session encryption
- B. Library control
- C. Input sanitization
- D. Removal of stored procedures

Answer: (SHOW ANSWER)

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies input sanitization as a primary countermeasure to prevent unauthorized database access from web applications. Input sanitization ensures that user-supplied data is validated, filtered, and escaped before being processed by backend systems.

CCISO materials emphasize that attacks such as SQL injection exploit unsanitized input fields to manipulate database queries. Sanitizing inputs prevents malicious commands from being executed by the database engine.

Session encryption protects data in transit but does not stop injection attacks. Library control and removing stored procedures do not address user input exploitation.

Therefore, input sanitization is the most effective and CCISO-aligned countermeasure.

NEW QUESTION: 53

When dealing with risk, the information security practitioner may choose to:

- A. assign
- B. transfer
- C. acknowledge
- D. defer

Answer: ([SHOW ANSWER](#))

Risk management options include transfer, which involves shifting the responsibility or cost of a risk to another party, typically through insurance or outsourcing.

* Options for Risk Management:

* Avoid: Eliminate the activity causing the risk.

* Mitigate: Reduce the risk to an acceptable level.

* Transfer: Pass the risk to another party.

* Accept: Acknowledge and tolerate the risk.

* Transfer in Practice:

* Commonly achieved via insurance or contracts with third-party providers.

* Alignment with Scenario:

* "Assign" and "Defer" are not standard risk responses. "Acknowledge" relates to acceptance, which is distinct from transferring risk.

* Risk Management Frameworks: Highlights transferring risk as a key strategy, particularly in business continuity and contractual agreements.

* Third-Party Risk Management: Demonstrates how outsourcing aligns with transferring risk responsibilities.

NEW QUESTION: 54

Which of the following is the MOST critical to review before you create a security strategy?

- A. Security industry technology trends
- B. The prior year security budget

C. Existing technology diagrams

D. The company business plan

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program clearly establishes that a security strategy must be business-driven, not technology-driven. As such, the most critical input before creating a security strategy is the company business plan.

CCISO documentation emphasizes that the role of the CISO is to enable and protect the business, not to build security in isolation. The business plan defines organizational objectives, growth strategies, market expansion, digital transformation initiatives, and risk tolerance. Without understanding these elements, a security strategy cannot be properly aligned or justified. Security technology trends (Option A) may inform tactical decisions later but do not define strategic priorities. The prior year budget (Option B) reflects historical spending, not future direction. Existing technology diagrams (Option C) are operational artifacts that support implementation, not strategy formation.

CCISO guidance consistently stresses that security strategy must support revenue generation, regulatory obligations, customer trust, and operational resilience. This alignment allows CISOs to clearly articulate value, secure executive sponsorship, and prioritize investments based on business risk.

Therefore, Option D is the correct answer.

NEW QUESTION: 55

Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.

When multiple regulations or standards apply to your industry you should set controls to meet the:

A. Easiest regulation or standard to implement

B. Stricter regulation or standard

C. Most complex standard to implement

D. Recommendations of your Legal Staff

Answer: ([SHOW ANSWER](#))

When multiple regulations or standards apply, the organization should adopt controls that comply with the stricter regulation or standard. This ensures compliance with all overlapping requirements and mitigates legal or financial risks.

* Understanding Regulatory Overlap:

* Industries like healthcare and finance often face multiple regulatory frameworks (e.g., GDPR, HIPAA, PCI DSS).

* Implementing stricter controls ensures that less stringent requirements are also met.

* Benefits of Choosing Stricter Standards:

* Minimizes risk of non-compliance across overlapping regulations.

* Future-proofs the organization as regulatory landscapes evolve.

* Role of Legal Recommendations:

- * While legal counsel provides valuable guidance, adhering to the strictest standard minimizes potential conflicts.
- * Compliance Management: Emphasizes implementing controls that exceed minimum requirements to address overlapping regulations effectively.
- * Risk Mitigation: Highlights the importance of adopting rigorous standards to avoid penalties and protect organizational reputation.

NEW QUESTION: 56

Acceptable levels of information security risk tolerance in an organization should be determined by?

- A. Corporate legal counsel
- B. CISO with reference to the company goals
- C. CEO and board of director
- D. Corporate compliance committee

Answer: ([SHOW ANSWER](#))

Determining Risk Tolerance

Acceptable levels of information security risk tolerance are a strategic decision that must align with the organization's overall risk appetite and business objectives.

- * The CEO and board of directors are responsible for setting the overall risk tolerance and ensuring it aligns with the organization's goals and compliance requirements.

Role of Other Entities

- * Corporate legal counsel: Provides legal guidance but does not set risk tolerance levels.
- * CISO with reference to company goals: Advises on technical risks and mitigations but does not make final decisions on risk tolerance.
- * Corporate compliance committee: Ensures adherence to regulatory requirements but doesn't determine organizational risk levels.

EC-Council References

- * EC-Council stresses the importance of executive-level involvement in establishing risk tolerance as part of governance and risk management frameworks.

NEW QUESTION: 57

A recommended method to document the respective roles of groups and individuals for a given process is to:

- A. Develop a detailed internal organization chart
- B. Develop a telephone call tree for emergency response
- C. Develop an isolinear response matrix with cost benefit analysis projections
- D. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart

Answer: ([SHOW ANSWER](#))

- * Explanation:

- * A RACI chart is a structured method to document the roles and responsibilities of individuals and groups in a process. It clarifies who is responsible, accountable, consulted, and informed for each task or decision.
- * This tool is widely used in project management and process optimization to eliminate ambiguity and ensure clear role delineation.
- * Why Other Options Are Incorrect:
 - * A. Organization chart: An org chart shows reporting relationships but does not document process-specific roles.
 - * B. Telephone call tree: A call tree is for communication during emergencies, not documenting roles in processes.
 - * C. Isolinear response matrix: This option is impractical and does not address role documentation.
- * EC-Council CISO Reference: The program emphasizes the use of tools like RACI charts to manage role clarity in IT security operations and projects.

NEW QUESTION: 58

A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding. Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

- A. The auditors have not followed proper auditing processes
- B. The CIO of the organization disagrees with the finding
- C. The risk tolerance of the organization permits this risk
- D. The organization has purchased cyber insurance

Answer: (SHOW ANSWER)

Risk Tolerance and Control Exceptions:

- * Organizations define their risk tolerance levels based on strategic objectives and resources.
- * If a risk is within acceptable tolerance, additional controls may not be necessary.

Why This is Correct:

- * The decision aligns with the organization's established risk management framework and priorities.

Why Other Options Are Incorrect:

- * A. Improper Audit Process: Unlikely; audits follow structured methodologies.
- * B. CIO Disagreement: Decisions are based on risk tolerance, not individual opinions.
- * D. Cyber Insurance: Mitigates financial loss but doesn't eliminate risk.

References:

EC-Council emphasizes that risk tolerance guides decisions on implementing controls, ensuring alignment with organizational objectives.

NEW QUESTION: 59

The process for identifying, collecting, and producing digital information in support of legal proceedings is called

- A. chain of custody.
- B. electronic discovery.
- C. evidence tampering.
- D. electronic review.

Answer: (SHOW ANSWER)

* Electronic discovery (e-discovery) involves identifying, collecting, and producing electronically stored information (ESI) as evidence in legal proceedings.

* This includes emails, documents, and other digital files relevant to the case.

Why Other Options Are Incorrect:

- * A. Chain of custody: Refers to the process of maintaining and documenting evidence handling.
- * C. Evidence tampering: Describes the illegal alteration of evidence, not the process of discovery.
- * D. Electronic review: Involves reviewing digital information but is part of the broader e-discovery process.

EC-Council CISO Reference:

Covers the importance of e-discovery in legal and compliance contexts, ensuring organizations are prepared to handle digital evidence properly.

NEW QUESTION: 60

What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

- A. Determine appetite
- B. Evaluate risk avoidance criteria
- C. Perform a risk assessment
- D. Mitigate risk

Answer: (SHOW ANSWER)

Steps in Risk Management According to NIST SP 800-30:

- * Step 1: Prepare for the risk management process.
- * Step 2: Perform a risk assessment to identify, evaluate, and prioritize risks.

Why Risk Assessment is the Second Step:

It provides a foundational understanding of the risks an organization faces, which informs subsequent steps like mitigation and monitoring.

Why Other Options Are Incorrect:

- * A. Determine appetite: Part of preparing, not the second step.
- * B. Evaluate avoidance criteria: Comes after assessing risks.
- * D. Mitigate risk: Happens after risks are assessed and prioritized.

References:

NIST SP 800-30 provides detailed guidance on performing risk assessments as an integral step in the risk management methodology.

NEW QUESTION: 61

The PRIMARY objective of security awareness is to:

- A. Ensure that security policies are read.
- B. Encourage security-conscious employee behavior.
- C. Meet legal and regulatory requirements.
- D. Put employees on notice in case follow-up action for noncompliance is necessary

Answer: (SHOW ANSWER)

Purpose of Security Awareness Programs:

The primary objective of security awareness initiatives is to foster a culture of security within the organization by educating employees on recognizing and responding to security risks.

Why Behavior Matters:

- * Educated employees act as a strong first line of defense against threats such as phishing and social engineering.
- * Awareness programs aim to integrate security-conscious behavior into daily workflows.

Why Other Options Are Incorrect:

- * A. Reading Policies: While important, it is not the primary focus of awareness programs.
- * C. Legal/Regulatory Requirements: Awareness contributes but is not solely for compliance.
- * D. Noncompliance Notice: Awareness is preventative, not primarily disciplinary.

References:

EC-Council prioritizes fostering secure behaviors as the core purpose of security awareness initiatives.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!
ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examd Discuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

When managing a project, the MOST important activity in managing the expectations of stakeholders is:

- A. To force stakeholders to commit ample resources to support the project
- B. To facilitate proper communication regarding outcomes
- C. To assure stakeholders commit to the project start and end dates in writing
- D. To finalize detailed scope of the project at project initiation

Answer: (SHOW ANSWER)

- * Managing Stakeholder Expectations:

- * Effective communication ensures stakeholders are informed about project goals, progress, and potential risks.
- * Clear and consistent communication builds trust and alignment with stakeholders' expectations.
- * Why Not Other Options:
- * A: Forcing resource commitment can lead to resistance and conflict.
- * C: Written commitment is useful but does not address ongoing expectation management.
- * D: Finalizing scope is important but secondary to continuous communication.

References:

* EC-Council CISO Handbook: Stakeholder Engagement and Communication in Project Management.

Reference: <https://www.greycampus.com/blog/project-management/stakeholder-management-what-is-it-and-why-is-it-so-important>

NEW QUESTION: 63

Of the following types of SOC (Security Operations Centers), which one would be MOST likely used if the CISO has decided to outsource the infrastructure and administration of it?

- A. Virtual
- B. Dedicated
- C. Fusion
- D. Command

Answer: (SHOW ANSWER)

A Virtual SOC (vSOC) is the most likely option when a CISO decides to outsource the infrastructure and administration of a Security Operations Center. vSOCs provide SOC services remotely through managed service providers, eliminating the need for in-house infrastructure while offering flexibility and scalability.

Dedicated SOC (B) are in-house setups, Fusion SOC (C) focus on cross-functional collaboration, and Command SOC (D) are typically centralized for large-scale operations.

Reference: <https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC>

NEW QUESTION: 64

Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?

- A. Upper management support
- B. More frequent project milestone meetings
- C. More training of staff members
- D. Involve internal audit

Answer: (SHOW ANSWER)

- * Upper management support is critical for removing obstacles, allocating necessary resources, and ensuring alignment with organizational priorities to bring delayed projects back on track.
- * Leadership buy-in often accelerates decision-making and reinforces project prioritization.

Why Other Options Are Less Effective:

- * B. More milestone meetings: Increased frequency of meetings can track progress but does not directly address root causes of delays.
- * C. More training: While valuable, training is not a short-term solution for project delays.
- * D. Involve internal audit: Audit ensures compliance and quality but is not typically involved in speeding up schedules.

EC-Council CISO Reference:

The curriculum highlights executive sponsorship as a pivotal factor in overcoming project challenges and ensuring timely completion.

NEW QUESTION: 65

Which of the following strategies provides the BEST response to a ransomware attack?

- A. Real-time off-site replication
- B. Daily incremental backup
- C. Daily full backup
- D. Daily differential backup

Answer: ([SHOW ANSWER](#))

Real-time off-site replication is the most effective response strategy for a ransomware attack because it ensures that up-to-date copies of data are continuously replicated to a secure, remote location. This allows for faster recovery with minimal data loss. Incremental, full, and differential backups (B, C, D) are valuable but may not provide the immediacy and recency of data recovery needed during ransomware incidents.

NEW QUESTION: 66

The rate of change in technology increases the importance of:

- A. Outsourcing the IT functions.
- B. Understanding user requirements.
- C. Hiring personnel with leading edge skills.
- D. Implementing and enforcing good processes.

Answer: ([SHOW ANSWER](#))

Importance of Processes Amid Technological Change

- * The rapid rate of technological innovation necessitates robust processes to adapt to emerging threats, compliance requirements, and operational changes.

Why Processes Are Critical

- * They ensure consistency, accountability, and efficiency in managing IT environments and security.
- * Good processes outlast changes in technology and personnel.

Comparison of Options

- * A. Outsourcing IT functions: May mitigate short-term challenges but doesn't address foundational needs.
- * B. Understanding user requirements: Important but secondary to enforcing processes.
- * C. Hiring personnel with leading-edge skills: Useful but insufficient without good processes.

EC-Council References

* EC-Council emphasizes the importance of process standardization (e.g., NIST CSF, ISO 27001) for sustained resilience.

NEW QUESTION: 67

An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors.

What is the MOST likely reason why the sensitive data was posted?

- A. The DLP Solution was not integrated with mobile device anti-malware
- B. Data classification was not properly performed on the assets
- C. The sensitive data was not encrypted while at rest
- D. A risk assessment was not performed after purchasing the DLP solution

Answer: ([SHOW ANSWER](#))

The most likely reason sensitive data was leaked despite the implementation of a DLP solution is inadequate data classification. Without proper classification, the DLP system cannot identify or apply appropriate controls to sensitive data. DLP solutions rely on predefined rules and policies tied to data labels; if sensitive data isn't accurately classified, it may not trigger protections.

Options A, C, and D address peripheral issues but do not explain the failure of the DLP system to detect and prevent the leak.

NEW QUESTION: 68

Which of the following is the MOST important goal of risk management?

- A. Identifying the risk
- B. Finding economic balance between the impact of the risk and the cost of the control
- C. Identifying the victim of any potential exploits.
- D. Assessing the impact of potential threats

Answer: ([SHOW ANSWER](#))

Goal of Risk Management:

* Risk management aims to optimize resources by finding a balance between the cost of implementing controls and the potential impact of the risks.

Decision-Making Framework:

* This ensures that controls are cost-effective and align with the organization's risk tolerance and business goals.

Supporting Reference:

* CCISO materials prioritize economic feasibility as a cornerstone of effective risk management.

NEW QUESTION: 69

One of the MAIN goals of a Business Continuity Plan is to

- A. Ensure all infrastructure and applications are available in the event of a disaster
- B. Allow all technical first-responders to understand their roles in the event of a disaster

- C. Provide step by step plans to recover business processes in the event of a disaster
- D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Answer: C (LEAVE A REPLY)

Purpose of a Business Continuity Plan (BCP):

- * The primary goal of a BCP is to ensure the continuity of critical business operations during and after a disaster.
- * CCISO materials emphasize the importance of documented, actionable recovery plans that outline procedures for maintaining essential services.

Focus on Process Recovery:

- * While infrastructure and applications are important, BCPs prioritize restoring business processes to maintain operational resilience.

Supporting Reference:

- * CCISO highlights the step-by-step recovery plans as a core component of a BCP, ensuring all stakeholders understand their roles and responsibilities.

NEW QUESTION: 70

Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand. You should:

- A. Create timelines for mitigation
- B. Develop a cost-benefit analysis
- C. Calculate annual loss expectancy
- D. Create a detailed technical executive summary

Answer: B (LEAVE A REPLY)

When communicating security priorities in business terms, a cost-benefit analysis helps explain the value of information resources and justifies security expenditures effectively to executives.

- * Understanding Executive Priorities:
 - * Executives focus on return on investment (ROI), cost efficiency, and alignment with business goals.
- * Cost-Benefit Analysis:
 - * Quantifies the benefits of protecting an asset versus the cost of implementing controls.
 - * Provides actionable insights for decision-makers.
- * Relevance of Other Options:
 - * Timelines and Executive Summaries do not provide the needed financial justification.
 - * Annual Loss Expectancy (ALE) is a metric but less comprehensive than a full cost-benefit analysis.
 - * Strategic Alignment: Emphasizes cost-benefit analysis for aligning security initiatives with business value.
 - * Risk Assessment and Prioritization: Stresses the need to communicate security impact in financial terms to executives.

NEW QUESTION: 71

When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

- A. Type of data contained in the process and system
- B. Type of connection and protocol used to transfer the data
- C. Type of encryption required for the data once it is at rest
- D. type of computer the data is processed on

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 72

A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

- A. Inability to export the private certificate/key
- B. It can double as physical identification at the DMV
- C. It has the user's photograph to help ID them
- D. It can be used as a secure flash drive

Answer: ([SHOW ANSWER](#))

* Key Cybersecurity Feature of a PIV Card:

* The PIV card securely stores a private key that cannot be exported, ensuring it is only used within the card itself.

* This prevents unauthorized access or duplication of sensitive cryptographic credentials.

* Why Not Other Options:

* B: While a PIV card might be used for physical identification, this is not its primary cybersecurity feature.

* C: A photograph helps with physical identification, but it is not a cybersecurity feature.

* D: PIV cards are not designed to function as secure flash drives.

References:

* SecureW2 Blog on PIV Features

* EC-Council CISO Handbook: Identity and Access Management.

Reference: <https://www.securew2.com/blog/piv-personal-identity-verification>

NEW QUESTION: 73

What is the PRIMARY weakness of a Cost Benefit Analysis (CBA)?

- A. It is not used very often
- B. It is not always precise
- C. It is not effective for mid-sized investments
- D. A positive result is an indication that the effort should be pursued

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies the primary weakness of Cost Benefit Analysis (CBA) as its lack of precision. While CBA is a valuable financial decision-making tool, CCISO materials stress that it often relies on estimates, assumptions, and probability-based inputs, particularly when applied to information security risks.

Security incidents are inherently uncertain, and factors such as threat likelihood, impact magnitude, and intangible costs (reputation damage, customer trust, regulatory scrutiny) are difficult to quantify accurately.

As a result, CBAs may produce results that appear mathematically sound but are based on imperfect data.

CCISO guidance emphasizes that CISOs must clearly communicate these limitations to executive leadership.

A positive CBA result does not guarantee success, nor does a negative result automatically justify rejection- especially for compliance-driven or risk-critical controls.

The other options do not reflect CCISO-identified weaknesses. CBAs are widely used, applicable to investments of all sizes, and positive results do not mandate pursuit.

Therefore, the correct and CCISO-aligned answer is It is not always precise.

NEW QUESTION: 74

Which of the following is a fundamental component of an audit record?

- A.** Date and time of the event
- B.** Failure of the event
- C.** Originating IP-Address
- D.** Authentication type

Answer: (SHOW ANSWER)

Fundamental Components of an Audit Record:

- * An audit record typically logs essential details of an event for tracking and accountability.
- * The date and time of the event are critical to correlate events and investigate incidents.

Why This is Correct:

- * Timestamping events ensures traceability and helps in forensic analysis.

Why Other Options Are Incorrect:

- * B. Failure of the event: This is a condition, not a fundamental component.
- * C. Originating IP-Address: Useful but not a core component.
- * D. Authentication type: Supplementary detail, not fundamental.

References:

EC-Council highlights the importance of accurate event timestamps in audit logs for monitoring and compliance.

NEW QUESTION: 75

Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

- A.** Segmentation controls.

- B. Shadow applications.
- C. Deception technology.
- D. Vulnerability management.

Answer: ([SHOW ANSWER](#))

* Definition of Deception Technology:

* Deception technology uses traps or decoys (e.g., fake environments or systems) to lure attackers away from critical assets.

* These decoys resemble legitimate systems and are designed to detect, contain, or study malicious activities.

* Functionality:

* Captures attacker behavior and methods without impacting real assets.

* Enables real-time alerts and forensic analysis while minimizing the attacker's ability to reach critical systems.

* Why Not Other Options:

* Segmentation controls: Restrict access to systems based on logical zones but do not actively lure attackers.

* Shadow applications: Refers to unauthorized or unmanaged software, not a security technology.

* Vulnerability management: Focuses on identifying and remediating vulnerabilities, not deception.

References:

EC-Council CISO Course: Advanced Threat Detection and Response Techniques.

NEW QUESTION: 76

A business unit within your organization intends to deploy a new technology in violation of information security standards. As a security leader, what would be your BEST course of action?

- A. Enforce the existing security standards and block deployment of the new system
- B. Assure that the standards align to the new system
- C. Create an exception for 6 months, then have the business request exception extensions
- D. Perform a risk analysis and provide the results to the business for a decision

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge stresses that the CISO's role is not to unilaterally block business initiatives, but to enable informed risk-based decision-making. When a business unit proposes technology that violates security standards, the best course of action is to perform a risk analysis and present the results to the business.

CCISO materials emphasize that risk ownership lies with the business, not the security function. The CISO is responsible for identifying, analyzing, and communicating risk-not for making business decisions.

Performing a risk analysis provides clarity on potential impacts, likelihood, regulatory exposure, and mitigation options.

Blocking deployment without analysis damages business alignment. Automatically granting exceptions undermines governance. Altering standards to fit technology weakens control frameworks.

Therefore, performing a risk analysis and enabling the business to make a risk-informed decision is the most effective and CCISO-aligned approach.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!
ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (**639** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 77

SCENARIO: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.

After determining the audit findings are accurate, which of the following is the MOST logical next activity?

- A. Begin initial gap remediation analyses
- B. Review the security organization's charter
- C. Validate gaps with the Information Technology team
- D. Create a briefing of the findings for executive management

Answer: (SHOW ANSWER)

Logical Next Activity After Validating Findings

- * Once gaps are validated, the logical next step is to perform remediation analyses to prioritize actions based on the severity of the gaps and available resources.
- * This step lays the groundwork for creating detailed remediation plans.

Why Not Other Options?

- * B. Review the security organization's charter: Not directly relevant to addressing audit findings.
- * C. Validate gaps with IT team: Validation is already complete at this stage.
- * D. Create a briefing for management: Comes after understanding the scope and potential impact of the gaps.

EC-Council References

- * Highlights gap remediation planning as a critical step post-validation to effectively address identified issues.

NEW QUESTION: 78

What is the MOST important reason to have senior leadership endorse security policies?

- A. Auditors will recognize the organization's commitment to security
- B. So they will accept ownership for security within the organization
- C. So that they can be held legally accountable when a severe incident occurs
- D. To force employees to adhere to security policies

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

CCISO documentation stresses that policy endorsement by senior leadership establishes ownership and accountability. When executives formally endorse policies, security becomes an organizational responsibility rather than a technical one.

While enforcement and audit recognition are benefits, CCISO materials emphasize that endorsement ensures leadership accepts responsibility for risk decisions and supports enforcement across the enterprise.

NEW QUESTION: 79

Which of the following statements below regarding Key Performance indicators (KPIs) are true?

- A. Development of KPI's are most useful when done independently
- B. They are a strictly quantitative measure of success
- C. They should be standard throughout the organization versus domain-specific so they are more easily correlated
- D. They are a strictly qualitative measure of success

Answer: (SHOW ANSWER)

* Key Performance Indicators (KPIs):

* KPIs are measurable values that demonstrate how effectively an organization is achieving key objectives.

* Standardization Importance:

* Uniform KPIs across the organization allow easy comparison, correlation, and alignment with overarching goals.

* Why Not Other Options:

* A: Independent development risks misalignment with strategic goals.

* B & D: KPIs can include both qualitative and quantitative metrics.

Reference:

KPI Development Guidelines: KPI.org

Reference: <https://kpi.org/KPI-Basics/KPI-Development>

NEW QUESTION: 80

The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

- A. Risk metrics
- B. Management metrics

C. Operational metrics

D. Compliance metrics

Answer: C ([LEAVE A REPLY](#))

Definition of Operational Metrics:

- * Operational metrics measure the day-to-day effectiveness of security processes and controls.
- * Examples include patching times, virus prevention rates, and vulnerability mitigation efforts.

Why This is Correct:

- * These metrics focus on operational activities that maintain security and efficiency.

Why Other Options Are Incorrect:

- * A. Risk Metrics: Measure potential risks, not operational activities.
- * B. Management Metrics: Focus on strategic outcomes, not daily operations.
- * D. Compliance Metrics: Measure adherence to regulations, not operational performance.

References:

EC-Council identifies metrics like mean time to patch and vulnerabilities mitigated as key operational metrics for maintaining security effectiveness.

NEW QUESTION: 81

Acme Inc. has engaged a third party vendor to provide 99.999% up-time for their online web presence and had them contractually agree to this service level agreement. What type of risk tolerance is Acme exhibiting?

(choose the BEST answer):

- A. low risk-tolerance**
- B. high risk-tolerance**
- C. moderate risk-tolerance**
- D. medium-high risk-tolerance**

Answer: ([SHOW ANSWER](#))

Risk Tolerance Definition:

- * A service level agreement (SLA) of 99.999% uptime indicates a very low tolerance for service interruptions or downtime.
- * This level of risk tolerance reflects an emphasis on high availability and minimal disruption, characteristic of organizations with critical online operations.

Why Other Options Are Incorrect:

- * B. High risk-tolerance: High risk-tolerance would reflect less stringent SLA requirements.
- * C. Moderate risk-tolerance: Moderate tolerance would accept more flexibility in uptime.
- * D. Medium-high risk-tolerance: This option does not accurately reflect the extreme precision of "five nines" uptime.

EC-Council CISO Reference:

The EC-Council CISO framework describes how SLAs and similar contractual agreements reflect organizational risk tolerance and strategic priorities.

NEW QUESTION: 82

What is the purpose of the statement of retained earnings of an organization?

- A.** It represents the sum of all capital expenditures
- B.** It represents the percentage of earnings that could in part be used to finance future security controls
- C.** It represents the savings generated by the proper acquisition and implementation of security controls
- D.** It has a direct correlation with the CISO's budget

Answer: ([SHOW ANSWER](#))

The statement of retained earnings shows the portion of net income retained by the organization after dividends are paid. These retained earnings can be reinvested in the company, such as financing security initiatives or technology upgrades. It does not directly correlate with capital expenditures (A), savings from security controls (C), or the CISO's budget (D).

NEW QUESTION: 83

During a cyber incident, which of the following non-security personnel will MOST likely be required to assist the incident response team?

- A.** Legal, help desk, system and network administrators
- B.** Threat analysts, IT auditors, security operations managers
- C.** Financial analysts, payroll clerks, HR managers
- D.** Human resources, facilities maintenance, and IT support

Answer: **A** ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program emphasizes that effective incident response is a cross-functional effort, extending well beyond the security team. During a cyber incident, the most critical non-security personnel required are legal counsel, help desk staff, and system/network administrators.

CCISO documentation explains that legal involvement is essential early in an incident to address regulatory notification requirements, liability exposure, evidence handling, and attorney-client privilege. System and network administrators are required to contain, isolate, restore, and validate affected systems, as they possess the technical authority and access needed for remediation actions. Help desk personnel play a key role in identifying user-reported issues, communicating instructions to staff, and supporting containment efforts such as password resets or endpoint isolation.

Option B consists entirely of security roles, not non-security personnel. Option C includes business roles that may be involved later but are not operationally critical during active incident response. Option D includes relevant teams, but facilities and HR are typically secondary unless the incident involves physical security or insider misconduct.

CCISO guidance aligns with NIST and ISO incident response frameworks, reinforcing that legal and IT operations are essential non-security partners in incident handling.

Therefore, Option A is correct.

NEW QUESTION: 84

Which security technologies are MOST critical to implementing a zero trust model?

- A. DLP, SIFM, IP5
- B. ACLs, secure gateways, IPS
- C. MFA, IAM, Endpoint Security
- D. Firewalls, IPS, WAF

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 85

Which organizational structure blends elements of functional and project organizational models to create a hybrid reporting structure?

- A. Distributed
- B. Sole owner
- C. Limited liability
- D. Matrix

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to the EC-Council CCISO Body of Knowledge, a matrix organizational structure is defined as a hybrid model that blends elements of both functional and project-based organizational structures. In a matrix structure, employees typically report to two authorities simultaneously: a functional manager (such as IT, security, or operations) and a project or program manager.

CCISO documentation highlights that matrix structures are commonly used in complex enterprises where resources must be shared across multiple initiatives without losing functional expertise. For CISOs, this structure is particularly relevant because information security initiatives often span multiple departments, including IT, legal, compliance, HR, and business units. The matrix model enables better collaboration while preserving accountability within functional domains.

The CCISO program emphasizes that while matrix structures improve flexibility and cross-functional alignment, they also introduce governance challenges, such as conflicting priorities, unclear authority, and resource contention. As a result, strong leadership, clearly defined roles, and executive sponsorship are required to prevent confusion and inefficiency.

The other options are not organizational reporting structures in the CCISO context. "Distributed" refers to system architecture, "sole owner" and "limited liability" describe business ownership/legal models, not internal organizational design.

Therefore, per CCISO governance and leadership principles, the correct answer is Matrix, as it uniquely combines functional and project-based reporting into a hybrid structure.

NEW QUESTION: 86

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?

- A.** International Organization for Standardizations - 22301 (ISO-22301)
- B.** Information Technology Infrastructure Library (ITIL)
- C.** Payment Card Industry Data Security Standards (PCI-DSS)
- D.** International Organization for Standardizations - 27005 (ISO-27005)

Answer: ([SHOW ANSWER](#))

Overview of ISO-22301:

ISO-22301 is the international standard for Business Continuity Management Systems (BCMS), providing a framework for ensuring continuity and disaster recovery.

Why This Standard is Best:

- * Offers specific guidance for developing and implementing consistent disaster recovery and business continuity processes.
- * Focuses on resilience, recovery, and business continuity across diverse business units.

Why Other Options Are Incorrect:

- * B. ITIL: Addresses IT service management, not business continuity.
- * C. PCI-DSS: Focuses on payment card security, not continuity.
- * D. ISO-27005: Focuses on risk management, not disaster recovery or business continuity.

References:

EC-Council recognizes ISO-22301 as the leading standard for creating robust disaster recovery and business continuity frameworks.

NEW QUESTION: 87

What is the purpose of a purple security testing team?

- A.** They defend against simulated hacker attacks during war gaming
- B.** They oversee security war-gaming exercises for performance reviews
- C.** They integrate defensive tactics with discovered threats and vulnerabilities
- D.** They emulate hackers to compromise systems within the network environment

Answer: **C** ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation:

CCISO documentation defines purple teams as a collaborative function that integrates red team (offensive) findings with blue team (defensive) improvements. Their purpose is to enhance detection, response, and resilience by sharing knowledge.

Red teams emulate attackers; blue teams defend. Purple teams integrate both. Therefore, option C is correct.

NEW QUESTION: 88

SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and

the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs.

The CISO discovers the scalability issue will only impact a small number of network segments. What is the next logical step to ensure the proper application of risk management methodology within the two-facto implementation project?

- A.** Create new use cases for operational use of the solution
- B.** Determine if sufficient mitigating controls can be applied
- C.** Decide to accept the risk on behalf of the impacted business units
- D.** Report the deficiency to the audit team and create process exceptions

Answer: ([SHOW ANSWER](#))

If the scalability issue impacts only a small number of network segments, the next logical step is to determine if sufficient mitigating controls can address the issue without replacing the entire solution.

* Risk Assessment:

* Identifies the extent of the issue and potential mitigation strategies.

* Considers controls to reduce the impact on affected segments.

* Risk Mitigation:

* If feasible controls exist, they can minimize risk while retaining the original solution.

* Other Options:

* A: Use cases are secondary to resolving the core issue.

* C: Risk acceptance should only occur after exploring mitigation options.

* D: Reporting deficiencies to audit is procedural but does not address the risk.

* Risk Mitigation Strategies: Prioritizes applying controls to reduce risks to acceptable levels.

* Incident and Problem Management: Emphasizes minimizing operational impact through mitigation.

Scenario8

NEW QUESTION: 89

When should IT security project management be outsourced?

- A.** When organizational resources are limited
- B.** When the benefits of outsourcing outweigh the inherent risks of outsourcing
- C.** On new, enterprise-wide security initiatives
- D.** On projects not forecasted in the yearly budget

Answer: ([SHOW ANSWER](#))

Outsourcing Decision Factors:

Outsourcing IT security project management can introduce risks, such as loss of control or confidentiality concerns. However, it is justified when the benefits, like cost savings, access to specialized expertise, or accelerated timelines, outweigh these risks.

Key Considerations for Outsourcing:

* Resource Constraints: Organizations may outsource when internal resources are unavailable or insufficient (A).

- * Budget and Strategy Fit: Projects outside the annual budget (D) might require outsourcing but only if risks are manageable.
- * Enterprise-wide Projects (C): These may involve critical risks, so outsourcing is considered only after thorough risk-benefit analysis.

EC-Council CISO Guidance:

The framework encourages assessing cost, risks, and security implications before outsourcing, ensuring alignment with strategic goals.

NEW QUESTION: 90

A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?

- A. Effective use of existing technologies
- B. Create a comprehensive security awareness program and provide success metrics to business units
- C. Proper budget management
- D. Leveraging existing implementations

Answer: (SHOW ANSWER)

Analyzing IT Infrastructure for Security

- * Ensuring that security solutions align with existing technologies demonstrates effective resource utilization and avoids unnecessary duplication of functionality.

Why Not Other Options?

- * B. Create a comprehensive security awareness program: Focuses on user behavior, not infrastructure analysis.
- * C. Proper budget management: Budgeting is essential but not the focus of infrastructure alignment.
- * D. Leveraging existing implementations: Overlaps with leveraging technology but lacks the broader focus of alignment and management.

EC-Council References

- * Stresses the importance of optimizing current IT and security resources before new implementations.

NEW QUESTION: 91

If a Virtual Machine's (VM) data is being replicated and that data is corrupted, this corruption will automatically be replicated to the other machine(s). What would be the BEST control to safeguard data integrity?

- A. Backup to tape
- B. Maintain separate VM backups
- C. Backup to a remote location
- D. Increase VM replication frequency

Answer: (SHOW ANSWER)

* Corruption Risk in Replication:

* Data corruption in one Virtual Machine (VM) is automatically replicated across other VMs due to the replication process. This makes relying solely on replication inadequate for safeguarding data integrity.

* Separate Backups:

* Maintaining separate VM backups ensures that corrupted or compromised data in the replicated environment can be recovered from an unaffected backup.

* These backups can be stored on a different storage medium or system to protect against widespread corruption.

* Best Practices:

* Regularly test the integrity of these backups.

* Implement a versioning system to ensure access to multiple historical copies.

Reference:

ISACA Journal on Backup and Recovery Practices: "Maintaining backups independent of replicated environments is critical to protect against data corruption scenarios." Reference: <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/is-audit-basics-backup-andrecovery>

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam! ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdisscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 92

A vendor delivering services refuses to make changes to work that is unsatisfactory and resulted in a failed quality test. Which of the following is the BEST course of action?

A. Submit a change request according to processes defined in the contract

B. Refer the issue to the legal department and ask for guidance

C. Withhold the vendor's payments until the issue is resolved

D. Quote the deliverables from the contract and insist that they make the changes

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program emphasizes that vendor management and third-party governance must be handled through contractual enforcement before escalation. When a vendor delivers work that fails quality testing and refuses to correct it, the first and best course of action is to reference the contractual obligations and enforce agreed-upon deliverables.

CCISO documentation stresses that contracts serve as the primary control mechanism for managing third-party risk. By quoting the specific deliverables, service levels, and acceptance criteria defined in the contract, the organization reinforces accountability without immediately escalating to legal action or punitive measures.

Submitting a change request (Option A) is inappropriate because the work is already contractually defined; the issue is non-compliance, not scope change. Withholding payment (Option C) may be contractually allowed but is typically a later enforcement step, not the first response. Referring the issue directly to legal counsel (Option B) is premature and contradicts CCISO guidance, which promotes structured escalation and governance maturity.

The CCISO curriculum highlights that effective CISOs resolve vendor issues through contractual governance, documentation, and formal communication, reserving legal remedies only when contractual enforcement fails.

Thus, Option D-quoting the deliverables and insisting on compliance-is the most appropriate, risk-aware, and governance-aligned action.

NEW QUESTION: 93

Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?

- A. Reviewing system administrator logs
- B. Auditing configuration templates
- C. Checking vendor product releases
- D. Performing system scans

Answer: ([SHOW ANSWER](#))

To effectively identify technical vulnerabilities, system scans are among the most effective methods. These scans can automatically detect security weaknesses in software, configurations, and systems. Tools like vulnerability scanners perform automated checks against databases of known vulnerabilities, ensuring comprehensive coverage across IT environments. While reviewing logs, auditing templates, and checking vendor releases contribute to overall security, scanning is both systematic and thorough in identifying vulnerabilities.

Reference: EC-Council CISO training materials on technical assessments and vulnerability scanning techniques.

NEW QUESTION: 94

Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

- A. Threat
- B. Vulnerability
- C. Attack vector
- D. Exploitation

Answer: ([SHOW ANSWER](#))

* Definition of Vulnerability:

- * A vulnerability is a weakness or gap in an asset that can be exploited by threats to cause harm.
- * Key Characteristics:
- * Vulnerabilities are the foundation for risk assessment and mitigation strategies, as they represent the exploitable points within an organization.
- * Supporting Reference:
- * EC-Council CCISO training defines vulnerability as a critical factor in understanding and addressing risks in security frameworks.

NEW QUESTION: 95

In what phase of an incident management process will malware antivirus signatures be distributed to infrastructure?

- A. Distribution
- B. Eradication
- C. Containment
- D. Collection

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The CCISO incident management lifecycle defines eradication as the phase in which malicious artifacts are removed and corrective actions are applied to prevent reinfection. This includes patching systems, removing malware, and distributing updated antivirus signatures.

CCISO guidance explains that containment focuses on limiting spread, collection focuses on evidence gathering, and distribution is not a formal incident phase. Antivirus signature updates are corrective measures designed to eliminate threats and prevent recurrence, making eradication the correct phase.

NEW QUESTION: 96

In defining a strategic security plan for an organization, what should a CISO first analyze?

- A. Reach out to a business similar to yours and ask for their plan
- B. Set goals that are difficult to attain to drive more productivity
- C. Review business acquisitions for the past 3 years
- D. Analyze the broader organizational strategic plan

Answer: ([SHOW ANSWER](#))

* Strategic Security Plan Foundation:

* The CISO must ensure that the security strategy aligns with the organization's broader strategic objectives.

* Analyzing the organizational strategic plan ensures that security initiatives support business goals, such as growth, innovation, or market expansion.

* Why Not Other Options:

* A: External plans may not align with internal goals or constraints.

* B: Unrealistic goals can lead to failure and misalignment with business objectives.

* C: Reviewing acquisitions is useful but not a starting point for strategic planning.

Reference:

SecurityIntelligence on Building Strategic Security Plans

Reference: <https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/>

NEW QUESTION: 97

An application vulnerability assessment has identified a security flaw in an application. This is a flaw that was previously identified and remediated on a prior release of the application. Which of the following is MOST likely the reason for this recurring issue?

- A. Ineffective configuration management controls
- B. Lack of change management controls
- C. Lack of version/source controls
- D. High turnover in the application development department

Answer: C (LEAVE A REPLY)

* Version/source control ensures that all code changes are tracked, and previously remediated flaws do not reappear.

* Without robust source control practices, outdated or insecure code can inadvertently be reintroduced.

Why Other Options Are Less Likely:

* A. Ineffective configuration management controls: This pertains to system configurations, not application code.

* B. Lack of change management controls: Change management addresses overall process but does not specifically prevent code reintroduction.

* D. High turnover in the development department: While turnover may contribute to the issue, the root cause is inadequate version/source control.

EC-Council CISO Reference:

Effective development practices, including version control, are emphasized as critical to maintaining application security.

NEW QUESTION: 98

Creating a secondary authentication process for network access would be an example of?

- A. Nonlinearities in physical security performance metrics
- B. Defense in depth cost enumerated costs
- C. System hardening and patching requirements
- D. Anti-virus for mobile devices

Answer: (SHOW ANSWER)

Layered Security Approach:

* Secondary authentication adds another layer of security, contributing to the Defense in Depth strategy.

* Enumerating costs ensures the layered approach is cost-effective and aligns with organizational budgets.

Why This is Correct:

* Secondary authentication strengthens access controls, a critical aspect of Defense in Depth.

Why Other Options Are Incorrect:

* A. Nonlinearities in metrics: Irrelevant to authentication processes.

* C. System hardening: Focuses on system configurations, not authentication.

* D. Anti-virus for mobile devices: Unrelated to authentication processes.

References:

EC-Council highlights Defense in Depth strategies as essential for layered protection mechanisms like secondary authentication.

NEW QUESTION: 99

You have been promoted to the CISO of a big-box retail store chain reporting to the Chief Information Officer (CIO). The CIO's first mandate to you is to develop a cybersecurity compliance framework that will meet all the store's compliance requirements.

Which of the following compliance standard is the MOST important to the organization?

A. The Federal Risk and Authorization Management Program (FedRAMP)

B. ISO 27002

C. NIST Cybersecurity Framework

D. Payment Card Industry (PCI) Data Security Standard (DSS)

Answer: (SHOW ANSWER)

For a big-box retail store chain, PCI DSS is the most critical compliance standard as it governs the security of cardholder data. Compliance ensures secure handling of payment transactions and reduces the risk of breaches, which could lead to financial and reputational damage. While ISO 27002 (B) and the NIST Cybersecurity Framework (C) provide general guidance, and FedRAMP (A) applies to government cloud service providers, PCI DSS specifically addresses the core compliance needs of retail businesses.

Reference: <https://searchcompliance.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard>

NEW QUESTION: 100

Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

A. Audit and Legal

B. Budget and Compliance

C. Human Resources and Budget

D. Legal and Human Resources

Answer: A (LEAVE A REPLY)

Formal Reporting Requirements:

* Information Security Governance programs must report to key organizational functions like Audit and Legal to ensure compliance, accountability, and alignment with regulatory requirements.

Role of Audit and Legal:

* Audit ensures program effectiveness, while Legal ensures compliance with applicable laws and manages risks of non-compliance.

Supporting Reference:

* CCISO training outlines these roles as critical stakeholders in formal reporting processes within governance frameworks.

NEW QUESTION: 101

Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.

Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?

- A. Scope
- B. Budget
- C. Resources
- D. Constraints

Answer: (SHOW ANSWER)

When a project is behind schedule and over budget, after verifying alignment with organizational goals, the next step is to verify the scope of the project. Scope creep or poorly defined scope is a common reason for delays and cost overruns.

* Why Verify Scope?:

* Ensures that the project's deliverables and objectives are clearly defined and aligned with expectations.

* Identifies any scope creep or additions not accounted for in the original plan.

* Impact of Scope Verification:

* Helps determine if the delays and overruns are due to changes in scope or lack of clarity.

* Provides a foundation for making adjustments to schedules, budgets, or resources.

* Other Factors:

* While budget, resources, and constraints are also critical, addressing the scope provides clarity on the root cause of project inefficiencies.

* Project Management Frameworks: Emphasizes scope management as a key step in addressing project delays.

* Best Practices in Project Oversight: Aligns scope verification with organizational goals and deliverables.

NEW QUESTION: 102

Which of the following is the MOST logical method of deploying security controls within an organization?

- A. Apply the least costly controls to demonstrate positive program activity

- B. Obtain funding for all desired controls and then create project plans for implementation
- C. Obtain business unit buy-in through close communication and coordination
- D. Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult and costly controls

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 103

A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?

- A. Alignment with the business
- B. Effective use of existing technologies
- C. Leveraging existing implementations
- D. Proper budget management

Answer: ([SHOW ANSWER](#))

* By analyzing the IT infrastructure and ensuring security solutions adhere to the principles of how hardware and software are implemented and managed, the CISO demonstrates effective use of existing technologies.

* This principle focuses on leveraging and optimizing current IT assets to maximize value and efficiency.

Why Other Options Are Less Relevant:

* A. Alignment with the business: This relates to ensuring security goals align with organizational objectives but is broader than analyzing infrastructure.

* C. Leveraging existing implementations: While related, this does not explicitly address management and implementation of hardware/software.

* D. Proper budget management: Budget management focuses on financial aspects, not technical alignment.

EC-Council CISO Reference:

Emphasizes the importance of maximizing existing technology investments as part of an efficient and secure IT strategy.

NEW QUESTION: 104

As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

- A. Executive summary
- B. Penetration test agreement
- C. Names and phone numbers of those who conducted the audit
- D. Business charter

Answer: ([SHOW ANSWER](#))

Purpose of an Executive Summary:

* An executive summary provides a high-level overview of the audit findings, making the report accessible to non-technical stakeholders, such as executives and board members.

Enhancing Audit Reports:

* Including detailed technical diagrams is important for specialists, but an executive summary bridges the gap by explaining the findings, risks, and recommendations in business terms.

Supporting Reference:

* CCISO materials recommend including executive summaries in reports to ensure alignment with organizational goals and executive decision-making processes.

NEW QUESTION: 105

What is the FIRST step in developing the vulnerability management program?

- A.** Baseline the Environment
- B.** Maintain and Monitor
- C.** Organization Vulnerability
- D.** Define Policy

Answer: (SHOW ANSWER)

The first step in developing a vulnerability management program is to define a policy, as it establishes the foundation for consistent and effective management of vulnerabilities.

* Define Policy:

* A policy outlines the organization's approach to identifying, evaluating, and addressing vulnerabilities. It includes scope, objectives, roles, and responsibilities.

* Baseline the Environment:

* After defining the policy, the current IT environment is assessed to identify existing vulnerabilities and benchmark security posture.

* Maintain and Monitor:

* Regular updates and monitoring are implemented to ensure the program remains effective over time.

* Organizational Vulnerability Awareness:

* Awareness activities follow the policy definition to align teams with organizational goals for vulnerability management.

* Implementation Order:

* Without a clear policy, efforts to baseline or maintain the environment may lack focus and consistency.

* Vulnerability Management Framework: Highlights the importance of establishing policies before operationalizing vulnerability scanning and remediation.

* Policy-Driven Security: EC-Council emphasizes the role of policies in aligning vulnerability management efforts with organizational goals and compliance requirements.

NEW QUESTION: 106

Which of the following is critical for a successful risk management program?

- A.** Accepting risk for regulatory compliance requirements

- B. Ensure developers include risk control comments in code
- C. Create risk assessment templates for every threat
- D. Provide risk visibility within the organization

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program stresses that risk visibility is essential for effective risk management.

Decision-makers must clearly understand what risks exist, their potential impact, and ownership.

Accepting regulatory risk (Option A) is generally inappropriate. Developer comments (Option B) and excessive templates (Option C) do not enable enterprise-wide decision-making.

CCISO governance principles emphasize that transparent risk communication enables informed business decisions, making Option D correct.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!

ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50

exam **questions have been updated** and **answers have been corrected** get the **newest**

ExamDiscuss.com 712-50 dumps with Test Engine here: [https://www.examd Discuss.com/EC-](https://www.examd Discuss.com/EC-COUNCIL/exam/712-50/premium/)

[COUNCIL/exam/712-50/premium/](https://www.examd Discuss.com/EC-COUNCIL/exam/712-50/premium/) (639 Q&As Dumps, **35%OFF** Special Discount Code:

freecram)

NEW QUESTION: 107

Which of the following are primary concerns for management with regard to assessing internal control objectives?

- A. Confidentiality, Availability, Integrity
- B. Compliance, Effectiveness, Efficiency
- C. Communication, Reliability, Cost
- D. Confidentiality, Compliance, Cost

Answer: (SHOW ANSWER)

Primary Concerns in Assessing Internal Control Objectives:

* Management evaluates whether controls ensure compliance with regulations, effectively mitigate risks, and operate efficiently.

Strategic Focus:

* These concerns help balance regulatory requirements, organizational objectives, and resource constraints.

Supporting Reference:

* CCISO highlights compliance, effectiveness, and efficiency as fundamental aspects of evaluating internal control objectives.

NEW QUESTION: 108

Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement's requirement for uptime?

- A. Systems logs
- B. Hardware error reports
- C. Utilization reports
- D. Availability reports

Answer: ([SHOW ANSWER](#))

Purpose of Availability Reports:

* Availability reports specifically track system uptime and service availability, making them the most relevant tool for verifying compliance with SLA requirements for uptime.

Alignment with SLA Objectives:

* These reports provide metrics and evidence needed to measure performance against agreed service levels.

Supporting Reference:

* CCISO materials emphasize using appropriate reporting tools like availability reports to validate compliance with service agreements.

NEW QUESTION: 109

How often should the SSAE16 report of your vendors be reviewed?

- A. Quarterly
- B. Semi-annually
- C. Annually
- D. Bi-annually

Answer: ([SHOW ANSWER](#))

SSAE 16 Report Overview:

SSAE 16 (Statement on Standards for Attestation Engagements) reports are used to assess a vendor's control environment and its alignment with security and compliance requirements.

Annual Review as Best Practice:

* Most vendors update their SSAE 16 reports annually, which reflects a complete cycle of operational and security practices.

* Reviewing the report annually ensures that the organization evaluates updated controls and addresses any identified risks.

Why Not Other Options:

* Quarterly (A) or semi-annual (B) reviews are excessive unless dictated by a high-risk environment.

* Bi-annual (D) review intervals may result in oversight of critical updates.

EC-Council Guidance:

Annual review aligns with standard compliance practices and maintains oversight of vendor security controls.

NEW QUESTION: 110

What key technology can mitigate ransomware threats?

- A. Use immutable data storage
- B. Phishing exercises
- C. Application of multiple end point anti-malware solutions
- D. Blocking use of wireless networks

Answer: ([SHOW ANSWER](#))

Immutable data storage protects against ransomware threats by ensuring that once data is written, it cannot be altered or deleted. This technology prevents ransomware from encrypting or modifying critical backups, enabling rapid restoration. Options B, C, and D are valuable for prevention and awareness but do not provide the direct protection against ransomware that immutable storage offers.

Reference: <https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent-ransomware-attacks>

NEW QUESTION: 111

What is the main purpose of the Incident Response Team?

- A. Ensure efficient recovery and reinstate repaired systems
- B. Create effective policies detailing program activities
- C. Communicate details of information security incidents
- D. Provide current employee awareness programs

Answer: ([SHOW ANSWER](#))

Purpose of the Incident Response Team:

* The primary goal of the IRT is to ensure a quick and efficient recovery from incidents while minimizing downtime and damage.

Recovery Focus:

* The IRT focuses on reinstating affected systems securely and ensuring operational continuity.

Supporting Reference:

* CCISO materials emphasize recovery and continuity as the main outcomes of incident response activities.

NEW QUESTION: 112

Which of the following uses encapsulation and encryption?

- A. Virtual Private Network (VPN)
- B. Virtual Local Area Network (VLAN)
- C. File Transfer Protocol (FTP)
- D. Simple Mail Transfer Protocol (SMTP)

Answer: A ([LEAVE A REPLY](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies a Virtual Private Network (VPN) as the technology that uses both encapsulation and encryption to secure communications across

untrusted networks. VPNs encapsulate original network packets inside an encrypted tunnel, protecting confidentiality, integrity, and authenticity of data in transit.

CCISO documentation explains that encapsulation allows private network traffic to be wrapped inside another protocol (such as IPsec or SSL/TLS), enabling secure transmission over public networks like the Internet.

Encryption ensures that even if traffic is intercepted, its contents cannot be read without the appropriate cryptographic keys.

A VLAN provides logical segmentation at Layer 2 but does not inherently encrypt traffic. FTP and SMTP transmit data in cleartext by default and provide neither encapsulation nor encryption unless additional secure variants (FTPS, SMTPS) are implemented.

CCISO materials emphasize that VPNs are a foundational control for remote access, site-to-site connectivity, and protection of sensitive data over external networks. Therefore, Virtual Private Network (VPN) is the correct answer.

NEW QUESTION: 113

Which control is used to discourage the exploitation of a vulnerability or system?

- A. Preventive
- B. Corrective
- C. Detective
- D. Deterrent

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words)

In the EC-Council CCISO framework, security controls are classified by their purpose and effect. A deterrent control is specifically designed to discourage or dissuade individuals from attempting to exploit a vulnerability, rather than technically blocking or detecting the attack.

CCISO materials define deterrent controls as those that influence human behavior through perceived consequences. Examples include warning banners, legal notices, security awareness messaging, visible surveillance, and sanctions policies. These controls do not stop attacks directly, nor do they detect or correct them; instead, they reduce the likelihood of exploitation by increasing perceived risk.

Preventive controls actively block threats (e.g., firewalls), detective controls identify incidents after occurrence (e.g., SIEM alerts), and corrective controls restore systems after an incident. None of these align with the concept of discouragement, which is explicitly tied to deterrence in CCISO documentation.

The CCISO program emphasizes that deterrent controls play a critical role in defense-in-depth strategies, particularly at the governance and policy level. They are especially effective against insider threats and opportunistic attackers.

Therefore, the correct answer is Option D: Deterrent.

NEW QUESTION: 114

What does the information security program primarily protect?

- A. All organizational assets as identified by the Chief Information Officer
- B. Audit schedules, reports, and remediations
- C. Critical data, systems, and processes
- D. Intellectual property and trademarks used by the business

Answer: C (LEAVE A REPLY)

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge defines the primary objective of an information security program as the protection of critical data, systems, and business processes that support organizational objectives.

CCISO guidance emphasizes that information security is a risk-based discipline, meaning not all assets are protected equally. Instead, resources are prioritized toward assets that are essential to mission execution, revenue generation, regulatory compliance, and operational resilience.

While intellectual property, trademarks, and other assets may be included, CCISO materials clarify that these are protected only insofar as they are critical to business operations. Similarly, audit artifacts and CIO-identified assets are not the primary focus of the security program itself. The CCISO framework highlights the CIA triad-confidentiality, integrity, and availability-as applied to critical information and systems, ensuring continuity and trust in business operations.

Therefore, the correct answer is critical data, systems, and processes.

NEW QUESTION: 115

The formal certification and accreditation process has four primary steps, what are they?

- A. Evaluating, describing, testing and authorizing
- B. Evaluating, purchasing, testing, authorizing
- C. Auditing, documenting, verifying, certifying
- D. Discovery, testing, authorizing, certifying

Answer: A (LEAVE A REPLY)

Steps in Certification and Accreditation

- * Evaluating: Assess security controls to identify gaps and areas of improvement.
- * Describing: Document the system, including security controls and configurations.
- * Testing: Perform validation testing to ensure controls meet security requirements.
- * Authorizing: Obtain formal approval to operate based on evaluation results and residual risk.

Comparison of Options

- * B. Evaluating, purchasing, testing, authorizing: Does not include describing, which is critical for documentation.
- * C. Auditing, documenting, verifying, certifying: Auditing and verifying are part of testing but are incomplete as standalone steps.
- * D. Discovery, testing, authorizing, certifying: Overlaps with evaluating but lacks specificity for describing.

EC-Council References

* Certification and accreditation frameworks (e.g., NIST RMF, ISO 27001) outline these steps for ensuring secure system authorization.

NEW QUESTION: 116

An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

- A.** A high threat environment
- B.** A low risk tolerance environment
- C.** A low vulnerability environment
- D.** A high risk tolerance environment

Answer: ([SHOW ANSWER](#))

Understanding Risk Tolerance:

* Choosing a less costly firewall with fewer capabilities, despite security concerns, indicates a willingness to accept higher risks. This reflects a high-risk tolerance environment.

Implications of the Decision:

* A high-risk tolerance approach prioritizes cost savings over robust security measures, which could lead to increased exposure to threats.

Supporting Reference:

* CCISO materials discuss how decisions on security investments reflect the organization's risk tolerance, balancing security needs with financial constraints.

NEW QUESTION: 117

A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

- A.** Compliance to the Payment Card Industry (PCI) regulations.
- B.** Alignment with financial reporting regulations for each country where they operate.
- C.** Alignment with International Organization for Standardization (ISO) standards.
- D.** Compliance with patient data protection regulations for each country where they operate.

Answer: ([SHOW ANSWER](#))

Industry-Specific Concerns:

* A global health insurance company handles sensitive patient data, making compliance with patient data protection laws (e.g., HIPAA in the U.S., GDPR in Europe) its primary concern.

Regulatory Compliance Focus:

* Different countries impose specific legal requirements to protect patient data. Failure to comply can lead to legal penalties and reputational harm.

Supporting Reference:

* CCISO training emphasizes the importance of adhering to applicable regulations for sensitive data in global operations to maintain compliance and trust.

NEW QUESTION: 118

Enforcing the implementation and management of security controls within services or products offered by third-party providers is a vital component of which security program service to the business?

- A. Vulnerability management
- B. Metrics and results enforcement
- C. Vendor management
- D. Security program governance

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, enforcing security controls in third-party services is a core function of vendor (third-party) management.

CCISO materials emphasize that vendor management ensures contractual security requirements, audits, attestations, and ongoing assurance. Vulnerability management (Option A) focuses internally. Governance (Option D) provides oversight but does not directly enforce vendor controls.

Therefore, Option C is correct.

NEW QUESTION: 119

As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

- A. File Transfer Protocol (FTP)
- B. Virtual Local Area Network (VLAN)
- C. Simple Mail Transfer Protocol
- D. Virtual Private Network (VPN)

Answer: ([SHOW ANSWER](#))

A Virtual Private Network (VPN) enables secure sharing of data by encapsulating and encrypting data packets over the network. VPNs create a secure "tunnel" between the organization and third parties, ensuring that data remains confidential and protected from unauthorized access during transmission. Other options like FTP, VLAN, and SMTP do not inherently provide the same level of encryption and secure encapsulation for extending network perimeters.

Reference: <https://searchnetworking.techtarget.com/definition/virtual-private-network>

NEW QUESTION: 120

Which of the following is MOST important when dealing with an Information Security Steering committee:

- A. Include a mix of members from different departments and staff levels.
- B. Ensure that security policies and procedures have been vetted and approved.
- C. Review all past audit and compliance reports.
- D. Be briefed about new trends and products at each meeting by a vendor.

Answer: (SHOW ANSWER)

Importance of Diverse Representation:

- * An effective Information Security Steering Committee should include representatives from various departments and organizational levels to ensure diverse perspectives and comprehensive decision-making.

Purpose of a Steering Committee:

- * To oversee security strategy, align it with business goals, and address risks across all operational areas.

Supporting Reference:

- * The CCISO program highlights cross-functional collaboration as a cornerstone of security governance to ensure balanced and inclusive security strategies.

NEW QUESTION: 121

In terms of supporting a forensic investigation, it is now imperative that managers, first-responders, etc., accomplish the following actions to the computer under investigation:

- A.** Secure the area and shut-down the computer until investigators arrive
- B.** Secure the area and attempt to maintain power until investigators arrive
- C.** Immediately place hard drive and other components in an anti-static bag
- D.** Secure the area.

Answer: (SHOW ANSWER)

- * Maintaining power ensures volatile memory (RAM) data is preserved, which can contain critical forensic evidence such as running processes and network connections.

- * Securing the area prevents tampering or unauthorized access, preserving the integrity of evidence.

Why Other Options Are Incorrect:

- * A. Shut-down the computer: Shutting down can result in loss of volatile data critical to the investigation.

- * C. Place components in anti-static bags: Prematurely removing hardware disrupts the state of the machine and can lead to loss of evidence.

- * D. Secure the area: While important, it does not address the need to preserve volatile memory.

EC-Council CISO Reference:

The first-responder guidelines stress the importance of preserving evidence integrity and avoiding actions that could destroy critical forensic data.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!
ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdisscuss.com/EC->

NEW QUESTION: 122

What are the four groups that are critical to the success of evaluating and approving contracts during the negotiation phase?

- A. Security, users, legal, marketing
- B. Legal, Finance, executives, users
- C. Security, executives, users, operations
- D. Legal, security, executives, users

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 123

The governing body that defines best practices for the collection of digital evidence is the:

- A. European Union (EU)
- B. National Institute of Standards and Technology (NI5T)
- C. Scientific Working Croup on Digital evidence (5WGDE)
- D. department of Defense (DoD)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 124

Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server. Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time. Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.

- A. Security Guards posted outside the Data Center
- B. Data Loss Prevention (DLP)
- C. Rigorous syslog reviews
- D. Intrusion Detection Systems (IDS)

Answer: ([SHOW ANSWER](#))

Best Technology for Preventing Data Exfiltration

- * DLP solutions monitor, detect, and prevent unauthorized data transfers, ensuring sensitive information does not leave the network.
- * DLP would have detected and blocked the analyst's attempt to upload data to a cloud service.

Why Not Other Options?

- * A. Security guards: Ineffective for digital data exfiltration.
- * C. Rigorous syslog reviews: Reactive, not preventive.
- * D. Intrusion Detection Systems (IDS): IDS focuses on detecting external threats, not internal data transfers.

EC-Council References

- * Highlights DLP as a critical tool for protecting sensitive data from unauthorized access and movement.

NEW QUESTION: 125

File Integrity Monitoring (FIM) is considered a

- A. Network based security preventative control
- B. Software segmentation control
- C. Security detective control
- D. User segmentation control

Answer: C (LEAVE A REPLY)

Definition of File Integrity Monitoring (FIM)

FIM is a security measure that detects unauthorized changes to files, configurations, or system settings. It logs and alerts administrators of anomalies, making it a key detective control.

Why FIM is a Detective Control

- * It does not prevent changes but monitors and reports them for further investigation.
- * Enhances visibility and auditability of system changes.

Comparison of Options

- * A. Network-based security preventative control: Preventative controls aim to block issues before they occur.
- * B. Software segmentation control: Refers to dividing software components, not monitoring.
- * D. User segmentation control: Focuses on access control policies for users, unrelated to file integrity.

EC-Council References

- * FIM is emphasized as a critical part of continuous monitoring and detection mechanisms in security frameworks taught by EC-Council.

NEW QUESTION: 126

What is the next step after defining the conditions under which standard security controls must be applied?

- A. Perform an asset inventory and apply classifications
- B. Analyze future security control plans
- C. Adopt a culture of risk awareness

D. Create risk mitigation plans

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

CCISO documentation explains that once conditions for applying controls are defined, the next step is to create risk mitigation plans. This translates control requirements into actionable remediation activities, timelines, and ownership.

Asset inventory and awareness are foundational steps that typically precede control definition. Therefore, risk mitigation planning follows control applicability.

NEW QUESTION: 127

Which of the following best describes a portfolio?

- A.** The portfolio is used to manage and track individual projects
- B.** The portfolio is used to manage incidents and events
- C.** A portfolio typically consists of several programs
- D.** A portfolio delivers one specific service or program to the business

Answer: ([SHOW ANSWER](#))

* Portfolio Definition:

* A portfolio is a collection of programs, projects, or operations managed collectively to achieve strategic objectives.

* It represents a higher-level grouping compared to individual projects or programs.

* Program vs. Portfolio:

* A program delivers a specific capability or service, whereas a portfolio manages multiple programs for alignment with organizational strategy.

* Key Characteristics of a Portfolio:

* It includes prioritization and resource allocation across various programs.

* Governance ensures alignment with business objectives.

References:

EC-Council CISO Module: Enterprise Governance and Portfolio Management.

NEW QUESTION: 128

What standard would you use to help define key performance indicators (KPIs)?

- A.** ITIL
- B.** GDPR
- C.** ISO 31000
- D.** NIST SP 800-55

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program explicitly references NIST SP 800-55 as the standard designed to support the development and use of performance measurement, including Key Performance Indicators (KPIs) and security metrics.

NIST SP 800-55 provides structured guidance on measuring the effectiveness and efficiency of security controls and programs. ITIL (Option A) addresses service management, GDPR (Option B) is a regulation, and ISO 31000 (Option C) focuses on enterprise risk management rather than performance metrics.

Thus, Option D is correct.

NEW QUESTION: 129

Risk appetite is typically determined by which of the following organizational functions?

- A. Security
- B. Business units
- C. Board of Directors
- D. Audit and compliance

Answer: ([SHOW ANSWER](#))

Role of the Board of Directors in Determining Risk Appetite:

The Board defines the organization's risk tolerance, balancing operational objectives with acceptable risk levels. This aligns with governance and fiduciary responsibilities.

Key Considerations:

- * Establishes strategic priorities and risk limits for the organization.
- * Ensures that risk management aligns with stakeholder expectations and regulatory requirements.

Why Not Other Options:

- * Security (A): Implements controls but does not set risk tolerance.
- * Business units (B): Manage operational risks but do not set overarching risk appetite.
- * Audit and compliance (D): Ensures adherence but does not define risk levels.

EC-Council Framework:

Governance and risk management frameworks emphasize the Board's role in defining and communicating risk appetite to guide organizational decision-making.

NEW QUESTION: 130

Risk transference is BEST represented by which of the following actions?

- A. Communicating the risk to all business units
- B. Outsourcing data storage operations to a third party
- C. Procuring cyber insurance
- D. Changing current processes for data retention

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge defines risk transference as shifting the financial impact of a risk to another party, while the risk itself still exists. The clearest and most common example of risk transference is procuring cyber insurance.

CCISO documentation explains that cyber insurance does not eliminate or reduce the likelihood of an incident; instead, it transfers the financial consequences-such as breach response costs, legal fees, and recovery expenses-to an insurer.

Outsourcing may shift operational responsibility but does not inherently transfer financial risk. Communication and process changes are examples of risk acceptance or mitigation, not transference.

Therefore, per CCISO risk treatment strategies, procuring cyber insurance best represents risk transference.

NEW QUESTION: 131

Why would you follow a formal risk management process in an organization that requires the use of Personally Identifiable Information (PII) as part of the business model?

- A.** To guarantee a successful risk transfer for handling this data
- B.** To clearly communicate the potential fines associated with using this type of data
- C.** To better analyze and communicate the business risks associated with this type of data
- D.** To determine if this type of data is necessary to the business

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program emphasizes that the primary purpose of formal risk management- especially when handling PII-is to analyze, quantify, and communicate business risk in a consistent and repeatable manner.

CCISO documentation explains that PII introduces legal, regulatory, operational, and reputational risks. A structured risk management process allows organizations to assess likelihood and impact, evaluate controls, and communicate risk exposure to executives and stakeholders in business terms.

Risk transfer (Option A) is one possible treatment option, not a guaranteed outcome.

Communicating fines (Option B) is only one aspect of risk and does not represent the full business impact. Determining whether data is necessary (Option D) may occur during data minimization discussions but is not the primary objective of risk management.

CCISO aligns risk management practices with ISO/IEC 27005 and enterprise risk management principles, reinforcing that effective decision-making requires clear risk communication.

Therefore, Option C is correct.

NEW QUESTION: 132

What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

- A.** Traffic Analysis
- B.** Deep-Packet inspection
- C.** Packet sampling
- D.** Heuristic analysis

Answer: ([SHOW ANSWER](#))

- * Deep-packet inspection (DPI) involves analyzing the content of packets in real-time as they traverse a network.
- * DPI can examine both headers and payloads of packets without introducing noticeable latency, making it suitable for real-time traffic monitoring.

Why Other Options Are Incorrect:

- * A. Traffic analysis: Focuses on metadata such as packet sizes, timing, and flow but does not inspect content.
- * C. Packet sampling: Involves analyzing only a subset of packets, potentially missing key information.
- * D. Heuristic analysis: Used for identifying patterns but does not specifically describe real-time deep inspection of packets.

EC-Council CISO Reference:

DPI is a critical technology discussed in advanced network security for monitoring and identifying malicious activity without impacting performance.

NEW QUESTION: 133

Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.

What action should you take FIRST?

- A. Destroy the repository of stolen data
- B. Contact your local law enforcement agency
- C. Consult with other C-Level executives to develop an action plan
- D. Contract with a credit reporting company for paid monitoring services for affected customers

Answer: (SHOW ANSWER)

Appropriate First Action After a Data Breach

- * Engaging law enforcement ensures proper handling of the breach within the legal framework, particularly when dealing with data stored on foreign servers.
- * Unauthorized actions, such as destroying data, may have legal repercussions and hinder investigations.

Why Not Other Options?

- * A. Destroy the repository of stolen data: Illegal and could result in evidence tampering.
- * C. Consult with C-Level executives: Important but secondary to legal compliance.
- * D. Contract with credit monitoring services: A remediation step that follows breach confirmation and law enforcement involvement.

EC-Council References

* Emphasizes involving legal authorities and following incident response procedures to ensure compliance.

NEW QUESTION: 134

Which of the following compliance standards is the MOST common among retail businesses?

- A.** Payment Card Industry (PCI) Data Security Standard (DSS)
- B.** NIST Cybersecurity Framework
- C.** Federal Risk and Authorization Management Program (FedRAMP)
- D.** ISO 27002

Answer: A ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program identifies PCI DSS as the most common compliance standard affecting retail organizations due to their handling of payment card data.

PCI DSS is mandatory for any organization that stores, processes, or transmits cardholder data.

CCISO materials emphasize that non-compliance can result in fines, loss of processing privileges, and reputational damage. NIST CSF (Option B) and ISO 27002 (Option D) are voluntary frameworks, while FedRAMP (Option C) applies only to U.S. federal cloud services. Therefore, Option A is correct.

NEW QUESTION: 135

In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

- A.** High risk environments 6 months, low risk environments 12 months
- B.** Every 12 months
- C.** Every 18 months
- D.** Every six months

Answer: ([SHOW ANSWER](#)**)**

Best Practices for Security Awareness Training:

Regular training ensures employees stay updated on emerging threats and reinforces secure behaviors.

International Standards and Practices:

* Most guidelines recommend annual training for all employees, regardless of the risk environment.

* High-risk environments may benefit from supplementary training, but the baseline remains 12 months.

Why Other Options Are Incorrect:

- * A. High-risk every 6 months: Not a standardized recommendation.
- * C. Every 18 months: Leaves gaps in awareness.
- * D. Every 6 months: Overly frequent and impractical for many organizations.

References:

EC-Council and other industry standards align with providing security awareness training every 12 months to maintain effectiveness and practicality.

NEW QUESTION: 136

You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget.

Using the best business practices for project management you determine that the project correct aligns with the company goals. What needs to be verified FIRST?

- A. Scope of the project
- B. Training of the personnel on the project
- C. Timeline of the project milestones
- D. Vendor for the project

Answer: (SHOW ANSWER)

When dealing with projects that are behind schedule and over budget, verifying the scope of the project is the first priority after ensuring alignment with company goals. A well-defined scope is essential for managing project timelines and budgets effectively.

* Scope Verification:

* Confirms that the project's deliverables are realistic, achievable, and clearly defined.

* Identifies deviations or expansions in scope (scope creep).

* Why Scope Comes First:

* Scope influences timelines, budgets, and resource needs.

* Ensures all stakeholders are aligned on project objectives.

* Other Options:

* Timeline, training, and vendor reviews are subsequent steps influenced by the scope.

* Project Management Best Practices: Recommends addressing scope first to resolve delays and budgetary issues.

* Risk Mitigation in Projects: Scope clarity reduces risks of overruns and inefficiencies.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!

ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 137

Which of the following is MOST likely to be discretionary?

- A. Policies

- B. Procedures
- C. Guidelines
- D. Standards

Answer: ([SHOW ANSWER](#))

Understanding Discretionary Elements:

- * Guidelines provide recommendations rather than mandatory actions. They are flexible and can be adapted based on specific circumstances.
- * Unlike policies, procedures, or standards, guidelines are not enforceable but are intended to support compliance with best practices.

Why Other Options Are Incorrect:

- * A. Policies: These are mandatory and must be adhered to.
- * B. Procedures: Step-by-step instructions that must be followed.
- * D. Standards: Define mandatory technical or procedural specifications.

References:

EC-Council recognizes guidelines as discretionary tools used to aid policy and procedure adherence without strict enforcement.

NEW QUESTION: 138

What function in an organization is responsible for collecting and communicating processes to facilitate the recovery of critical functions within an organization?

- A. Business Continuity
- B. Disaster Recovery
- C. Security Operations
- D. Legal Advisement

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to the EC-Council CCISO Body of Knowledge, Business Continuity is the organizational function responsible for collecting, documenting, and communicating processes required to ensure the recovery of critical business functions following a disruption.

CCISO documentation explains that Business Continuity focuses on people, processes, facilities, and workflows, ensuring that essential services continue or resume within acceptable timeframes.

This includes developing Business Continuity Plans (BCPs), conducting Business Impact Analyses (BIAs), and coordinating recovery strategies across departments.

Disaster Recovery is a subset of Business Continuity and focuses primarily on IT systems and infrastructure recovery, not the broader business processes. Security Operations manages day-to-day threat monitoring, while legal advisement supports compliance and legal matters.

CCISO materials emphasize that effective Business Continuity requires cross-functional coordination and clear communication so that employees understand their roles during disruptions.

Therefore, Business Continuity is the correct answer.

NEW QUESTION: 139

What is a critical initial step when creating a Business Continuity Plan (BCP)?

- A. Conduct a full risk assessment on all business operations and technologies
- B. Create multiple layers of process steps
- C. Conduct a Business Impact Analysis (BIA)
- D. Define accurate Recovery Point Objectives (RPOs) and regularly test them

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge clearly identifies the Business Impact Analysis (BIA) as the critical initial step in the creation of a Business Continuity Plan (BCP). CCISO documentation emphasizes that without first understanding how disruptions affect business operations, any continuity planning effort would lack strategic direction and measurable priorities. A BIA is used to identify and evaluate the potential effects of disruptions to critical business functions.

According to CCISO guidance, the BIA determines which processes are essential, the maximum tolerable downtime (MTD), and the operational and financial impacts associated with system outages, data loss, or service interruptions. This analysis provides executive leadership with visibility into which assets, systems, and processes must be prioritized for continuity and recovery.

While risk assessments are important, CCISO distinguishes them from BIAs by stating that risk assessments focus on threat likelihood and vulnerabilities, whereas BIAs focus on business consequences. CCISO materials explicitly note that a BIA must be completed before defining recovery strategies, selecting controls, or establishing recovery objectives such as RPOs and RTOs.

Options such as creating layered process steps or defining RPOs are considered subsequent activities that rely on the findings of the BIA. CCISO frameworks stress that recovery objectives cannot be accurately defined without first understanding business impact. Therefore, conducting a BIA serves as the foundation upon which the entire BCP lifecycle is built.

In summary, the CCISO program confirms that conducting a Business Impact Analysis (BIA) is the most critical and correct initial step when developing a Business Continuity Plan.

NEW QUESTION: 140

What does an anonymous network consist of as the PRIMARY supporting components?

- A. Volunteer computers
- B. Covert databases
- C. Discrete networks
- D. War driving maps

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program explains that anonymous networks-such as Tor-are primarily supported by volunteer-operated computers (nodes) distributed globally. These volunteer systems relay traffic to obscure the origin, destination, and identity of users.

CCISO documentation highlights that anonymity is achieved through traffic routing and encryption, not proprietary infrastructure or hidden databases. Covert databases (Option B) and discrete networks (Option C) are not defining components of anonymous networks. War driving maps (Option D) are unrelated to anonymity technologies.

Understanding anonymous network infrastructure is important for CISOs when assessing threats related to data exfiltration, command-and-control communications, and threat actor anonymity.

Therefore, Option A is the correct answer.

NEW QUESTION: 141

When managing the critical path of an IT security project, which of the following is MOST important?

- A.** Knowing who all the stakeholders are.
- B.** Knowing the people on the data center team.
- C.** Knowing the threats to the organization.
- D.** Knowing the milestones and timelines of deliverables.

Answer: (SHOW ANSWER)

Critical Path in IT Security Projects:

The critical path represents the sequence of tasks that determine the overall project duration. Managing this requires a clear understanding of milestones and timelines to ensure that deliverables are completed on schedule.

Why Milestones and Timelines Are Crucial:

- * Project Monitoring: Provides the ability to track progress and make adjustments as necessary.
- * Dependency Management: Ensures that tasks dependent on others are completed in the correct sequence.
- * Risk Mitigation: Identifies bottlenecks that could delay the entire project.

Why Not Other Options:

- * Stakeholder knowledge (A) is important but secondary to understanding critical deliverables.
- * Data center team familiarity (B) may be useful but isn't the key to managing a project's critical path.
- * Threat knowledge (C) is more relevant to the security strategy than project execution.

EC-Council CISO Alignment:

Effective project management requires focus on timelines and milestones to ensure security objectives are met within the designated timeframe.

NEW QUESTION: 142

The Information Security Management program MUST protect:

- A.** all organizational assets
- B.** critical business processes and /or revenue streams

- C. intellectual property released into the public domain
- D. against distributed denial of service attacks

Answer: ([SHOW ANSWER](#))

Focus of Information Security Management Programs:

The primary goal is to protect critical business processes and revenue streams by ensuring the confidentiality, integrity, and availability of information assets.

Why This is Correct:

- * Business processes and revenue are at the heart of organizational operations.
- * The security management program prioritizes assets that directly impact these areas.

Why Other Options Are Incorrect:

- * A. All organizational assets: Impractical and not prioritized equally.
- * C. Intellectual property released into the public domain: Less critical once public.
- * D. Against DDoS attacks: Part of the scope but not the main focus.

References:

EC-Council emphasizes that protecting critical business operations is the cornerstone of an effective Information Security Management program.

NEW QUESTION: 143

Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

- A. Poses a strong technical background
- B. Understand all regulations affecting the organization
- C. Understand the business goals of the organization
- D. Poses a strong auditing background

Answer: ([SHOW ANSWER](#))

Aligning Security with Organizational Culture:

Security leaders must align security initiatives with business objectives to gain stakeholder support and integrate security into daily operations effectively.

Key Traits of Security Leaders:

- * Business acumen to link security practices with organizational goals.
- * The ability to communicate security's value in enabling business success.

Why Other Options Are Incorrect:

- * A. Technical Background: Helpful but not sufficient for cultural influence.
- * B. Understanding Regulations: Essential but secondary to business alignment.
- * D. Auditing Background: Supports governance but does not directly influence culture.

References:

EC-Council emphasizes that understanding business goals is crucial for CISOs to align security with organizational priorities effectively.

NEW QUESTION: 144

You have been promoted to the CISO of a retail store. Which of the following compliance standards is the MOST important to the organization?

- A. Payment Card Industry (PCI) Data Security Standard (DSS)
- B. ISO 27002
- C. NIST Cybersecurity Framework
- D. The Federal Risk and Authorization Management Program (FedRAMP)

Answer: ([SHOW ANSWER](#))

For a retail store, compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) is crucial, as it governs the secure handling of cardholder data and ensures the safety of payment transactions. ISO

27002 (B) and the NIST Cybersecurity Framework (C) offer general guidelines, while FedRAMP (D) applies to government cloud services, making them less critical to retail-specific compliance needs.

NEW QUESTION: 145

What type of test is performed by an auditor when a sample of programs is selected to determine if software source and object versions are the same?

- A. A sample test of program library features
- B. A sample test of programming object reuse controls
- C. A compliance test of program compiler operations
- D. A compliance test of program library controls

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, verifying that source code and compiled object code match is part of a compliance test of program library controls.

Program library controls ensure that only authorized, approved, and properly compiled code is promoted to production. Auditors test these controls to confirm integrity, version control, and change management effectiveness.

Compiler operations (Option C) relate to build processes, not library integrity. Options A and B do not address compliance verification. Therefore, Option D is correct.

NEW QUESTION: 146

You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?

- A. Validate that security awareness program content includes information about the potential vulnerability
- B. Conduct a thorough risk assessment against the current implementation to determine system functions
- C. Determine program ownership to implement compensating controls
- D. Send a report to executive peers and business unit owners detailing your suspicions

Answer: ([SHOW ANSWER](#))

Risk Assessment as a Best Practice:

EC-Council CISO stresses that suspected vulnerabilities, especially in critical systems like two-factor authentication, require an immediate and thorough risk assessment. This ensures that risks are quantified and mitigation efforts are appropriately prioritized.

Steps in the Process:

- * Conduct a detailed assessment of the token management process.
- * Identify vulnerabilities, potential exploitation scenarios, and system dependencies.
- * Assess the impact of the flaw on the organization's security posture.

Why Not Other Options:

- * Security awareness (A) is important but doesn't address the root technical issue.
- * Reporting suspicions (D) is premature without substantiating evidence.
- * Determining program ownership (C) is part of the response plan but not the first step.

CISO Alignment:

This approach ensures a proactive, measured, and evidence-driven resolution to the issue.

NEW QUESTION: 147

Which type of scan is used on the eye to measure the layer of blood vessels?

- A. Retinal scan
- B. Signature kinetics scan
- C. Facial recognition scan
- D. Iris scan

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 148

The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong?

(choose the BEST answer):

- A. Deployed the encryption solution in an inadequate manner
- B. Used hardware encryption instead of software encryption
- C. Used 1024 bit encryption when 256 bit would have sufficed
- D. Failed to identify all stakeholders and their needs

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 149

The alerting, monitoring and life-cycle management of security related events is typically handled by the

- A. security threat and vulnerability management process

- B. risk assessment process
- C. risk management process
- D. governance, risk, and compliance tools

Answer: ([SHOW ANSWER](#))

Role of Threat and Vulnerability Management:

- * This process focuses on detecting, assessing, and addressing threats and vulnerabilities in real-time, ensuring timely response to security events.
- * It includes continuous monitoring, alerting, and incident lifecycle management.

Alerting and Monitoring:

- * The CCISO program outlines how threat and vulnerability management tools integrate with security monitoring systems to provide situational awareness and proactive defense mechanisms.

Supporting Reference:

- * CCISO materials explain the lifecycle approach to security event management, where threat management processes play a pivotal role in incident detection and remediation.

NEW QUESTION: 150

Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

- A. Incident response plan
- B. Business Continuity plan
- C. Disaster recovery plan
- D. Damage control plan

Answer: ([SHOW ANSWER](#))

Disaster Recovery Plan (DRP):

- * A DRP provides detailed, step-by-step procedures for restoring systems and operations after a disaster, such as a major earthquake. The focus is on IT systems and critical infrastructure.

Comparison with Other Plans:

- * While a Business Continuity Plan (BCP) addresses broader organizational operations, the DRP specifically targets technical recovery.

Supporting Reference:

- * CCISO materials highlight DRP as the primary tool for regaining IT operational normalcy after a disaster.

NEW QUESTION: 151

If your organization operates under a model of "assumption of breach", you should:

- A. Protect all information resource assets equally
- B. Establish active firewall monitoring protocols
- C. Purchase insurance for your compliance liability
- D. Focus your security efforts on high value assets

Answer: ([SHOW ANSWER](#))

Assumption of Breach Model:

* This model assumes that breaches are inevitable, emphasizing proactive defense and focusing resources on protecting critical assets.

High-Value Asset Focus:

* Critical data and systems are prioritized to minimize the impact of a breach and ensure business continuity.

Supporting Reference:

* The CCISO framework recommends prioritizing high-value assets as part of a risk-based security strategy under the assumption of breach model.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam! ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examd Discuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 152

Which of the following provides the BEST software risk remediation methods?

- A. Software removal, define requirements, install updates
- B. Discover software, deploy integrations, apply updates
- C. Install patches and updates, adjust configurations, remove software
- D. Install software replacements, remove data, maintain system

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program defines effective software risk remediation as actions that reduce exposure by eliminating vulnerabilities and unnecessary attack surface. The most effective remediation methods are installing patches and updates, adjusting configurations, and removing unnecessary or unsupported software.

CCISO documentation emphasizes that vulnerabilities are most commonly addressed through patch management, secure configuration, and software decommissioning. Adjusting insecure default configurations and removing obsolete software directly reduce exploitable weaknesses. Other options either include non-remediation activities (defining requirements, discovering software) or incomplete approaches that do not fully address risk. CCISO aligns remediation best practices with NIST and ISO vulnerability management guidance.

Therefore, Option C is correct.

NEW QUESTION: 153

Which of the following is a metric used for data backup and restoration metrics?

- A. Mean Time to Operations (MTO)

- B. Recovery Base Objective (RBO)**
- C. Maximum Tolerable Downtime (MTD)**
- D. Recovery Point Objective (RPO)**

Answer: D ([LEAVE A REPLY](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies Recovery Point Objective (RPO) as a key metric used specifically for data backup and restoration. RPO defines the maximum acceptable amount of data loss, measured in time, that an organization can tolerate following a disruption or system failure.

CCISO documentation explains that RPO answers the question: "How much data can we afford to lose?" This makes it directly tied to backup frequency, replication strategies, and data restoration planning. For example, an RPO of four hours means backups must occur at least every four hours to meet business requirements.

Other options are related but not specific to backup metrics. Maximum Tolerable Downtime (MTD) measures total allowable downtime for a business process, not data loss. Mean Time to Operations (MTO) focuses on recovery duration. "Recovery Base Objective" is not a recognized CCISO or industry-standard metric.

CCISO materials emphasize that defining RPO is critical before selecting backup technologies, cloud replication methods, or disaster recovery architectures. Without a clearly defined RPO, organizations risk either over-investing in unnecessary backup solutions or under-protecting critical data.

Therefore, in alignment with CCISO business continuity and disaster recovery guidance, Recovery Point Objective (RPO) is the correct answer.

NEW QUESTION: 154

A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat. This is an example of:

- A. Change management**
- B. Business continuity planning**
- C. Security Incident Response**
- D. Thought leadership**

Answer: ([SHOW ANSWER](#))

* Convening key stakeholders to address a severe security threat is a classic example of a security incident response. It involves analyzing the threat, determining modifications to security controls, and mitigating the risk to the organization.

Why Other Options Are Incorrect:

* A. Change management: Change management refers to processes for systematic and planned modifications, not rapid responses to urgent threats.

- * B. Business continuity planning: This focuses on maintaining critical operations during disruptions, not responding to immediate security incidents.
- * D. Thought leadership: This pertains to driving strategic innovation or expertise, not operational incident response.

EC-Council CISO Reference:

The incident response lifecycle, as outlined in the EC-Council program, stresses the importance of prompt coordination and action during security threats.

NEW QUESTION: 155

Which of the following is the MOST important for a CISO to understand when identifying threats?

- A. How vulnerabilities can potentially be exploited in systems that impact the organization
- B. How the security operations team will behave to reported incidents
- C. How the firewall and other security devices are configured to prevent attacks
- D. How the incident management team prepares to handle an attack

Answer: ([SHOW ANSWER](#))

Understanding Threats:

- * A CISO must comprehend how vulnerabilities in organizational systems can be exploited by threats to effectively prioritize risk management efforts.

Key Focus:

- * This knowledge helps in implementing targeted security measures to protect critical systems and data.

Supporting Reference:

- * CCISO materials highlight the importance of understanding the threat landscape and its relation to vulnerabilities to anticipate and mitigate potential exploits.

NEW QUESTION: 156

What organizational structure combines the functional and project structures to create a hybrid of the two?

- A. Traditional
- B. Composite
- C. Project
- D. Matrix

Answer: ([SHOW ANSWER](#))

Matrix Structure Overview:

- * Combines functional and project structures to create a hybrid, allowing employees to report to both functional managers and project managers.
- * Balances resource allocation and functional expertise with project focus.

Comparison with Other Options:

- * A: Traditional structures focus solely on functional hierarchy.
- * B: Composite structures may blend multiple styles but are not as focused on functional-project integration.

* C: Project struct

CCCCC

Reference: <https://www.knowledgehut.com/tutorials/project-management/organization-structures>

NEW QUESTION: 157

What term BEST describes assuring the actions of employees, applications, and systems follow the organization's rules and regulations?

- A. Asset functionalization
- B. Compliance management
- C. Risk management
- D. Audit checklist

Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation:

According to CCISO governance principles, compliance management ensures that people, processes, applications, and systems adhere to internal policies and external regulatory requirements. Risk management identifies and prioritizes risks, while audits verify compliance-but compliance management ensures ongoing adherence.

NEW QUESTION: 158

What is the first action taken when reacting to a malware attack?

- A. Recovery
- B. Escalation
- C. Eradication
- D. Containment

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to CCISO incident response guidance, containment is the first action taken when reacting to a malware attack. CCISO materials explain that the immediate priority is to limit spread and impact by isolating affected systems, disabling compromised accounts, or blocking malicious traffic.

Eradiation and recovery occur later in the lifecycle, after containment is achieved. Escalation may occur concurrently, but containment is the first technical response action to protect the organization.

NEW QUESTION: 159

How often should an environment be monitored for cyber threats, risks, and exposures?

- A. Weekly
- B. Monthly
- C. Quarterly
- D. Daily

Answer: (SHOW ANSWER)

Cyber Threat Monitoring Frequency:

- * Continuous monitoring or daily checks are essential to detect and mitigate threats promptly.
- * Cyber environments are dynamic, with risks emerging in real time.

Why This is Correct:

- * Daily monitoring ensures timely detection and response to vulnerabilities, intrusions, or unusual activities.

Why Other Options Are Incorrect:

- * A. Weekly, B. Monthly, C. Quarterly: Insufficient for detecting rapidly evolving cyber threats.

References:

EC-Council emphasizes daily monitoring as a critical component of proactive cybersecurity operations.

NEW QUESTION: 160

Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

- A. Risk Management
- B. Risk Assessment
- C. System Testing
- D. Vulnerability Assessment

Answer: (SHOW ANSWER)

Role of Risk Assessment:

Risk assessment evaluates potential risks associated with IT initiatives or systems by identifying vulnerabilities, threats, and their potential impacts. This process informs the implementation of an information security program.

Key Actions:

- * Assess threats and vulnerabilities.
- * Determine the likelihood and impact of risks.
- * Prioritize risks for mitigation.

Why Not Other Options:

- * Risk Management (A): Oversees the broader risk mitigation process but does not focus solely on evaluation.
- * System Testing (C): Verifies technical functionality but does not assess risks holistically.
- * Vulnerability Assessment (D): Focuses narrowly on technical weaknesses, not comprehensive risk evaluation.

EC-Council Emphasis:

Risk assessment is foundational to evaluating and addressing risks effectively in security programs.

NEW QUESTION: 161

An organization has decided to develop an in-house BCM capability. The organization has determined it is best to follow a BCM standard published by the International Organization for Standardization (ISO).

The BEST ISO standard to follow that outlines the complete lifecycle of BCM is?

- A. ISO 22318 Supply Chain Continuity
- B. ISO 27031 BCM Readiness
- C. ISO 22301 BCM Requirements
- D. ISO 22317 BIA

Answer: ([SHOW ANSWER](#))

ISO 22301 provides a comprehensive standard for Business Continuity Management (BCM) requirements, covering the complete BCM lifecycle, including planning, implementing, operating, monitoring, and improving BCM systems. While ISO 22318 (A) focuses on supply chain continuity and ISO 27031 (B) addresses ICT readiness, ISO 22301 offers a broader approach. ISO 22317 (D) pertains specifically to Business Impact Analysis (BIA).

Reference: <https://www.smartsheet.com/content/iso-22301-business-continuity-guide>

NEW QUESTION: 162

A digital signature addresses which of the following concerns?

- A. Message alteration
- B. Message copying
- C. Message theft
- D. Unauthorized reading

Answer: ([SHOW ANSWER](#))

A digital signature ensures the integrity and authenticity of a message by verifying that the content has not been altered during transmission. It uses cryptographic techniques to create a unique hash for the message, which is encrypted using the sender's private key. The recipient can decrypt this hash using the sender's public key and compare it to the computed hash of the received message. If the hashes match, the message remains unaltered, addressing the concern of message alteration.

Reference: <https://www.entrust.com/resources/certificate-solutions/learn/digital-signatures>

NEW QUESTION: 163

Which of the following would be used to measure the effectiveness of an Information Security Management System (ISMS)?

- A. Information Technology Infrastructure Library (ITIL)
- B. Control Objectives for Information and Related Technology (COBIT)
- C. International Organization for Standardization (ISO) 27004
- D. International Organization for Standardization (ISO) 27005

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

Exact alignment with EC-Council CCISO documentation and referenced ISO standards According to EC-Council Chief Information Security Officer (CCISO) program documentation, measuring the effectiveness of an Information Security Management System (ISMS) requires defined, repeatable, and standardized metrics. The CCISO body of knowledge explicitly aligns ISMS performance measurement with ISO/IEC 27004, which is the international standard dedicated to information security metrics, measurement, and reporting.

ISO/IEC 27004 provides guidance on how organizations should develop, implement, analyze, and improve measurements that assess the effectiveness and efficiency of an ISMS. The CCISO program emphasizes that governance-level leaders must rely on quantifiable, objective metrics rather than operational frameworks or risk assessment standards when evaluating ISMS performance. ISO 27004 directly supports this executive requirement by defining what to measure, how to measure it, and how to interpret results in the context of business objectives. In contrast, ITIL is a service management framework focused on IT service delivery and lifecycle management, not on measuring ISMS effectiveness. While ITIL supports operational excellence, CCISO materials clearly distinguish IT service management from security governance measurement.

COBIT (corrected from the incorrect spelling "CODIT") is a governance and management framework for enterprise IT. Although COBIT includes security-related control objectives and maturity models, it is not designed specifically to measure ISMS effectiveness at the level required by ISO-aligned security programs.

ISO/IEC 27005, meanwhile, focuses on information security risk management. The CCISO curriculum explains that risk assessment is a critical component of an ISMS, but it does not provide guidance on performance measurement or effectiveness metrics.

Therefore, as confirmed in EC-Council CCISO documentation and its reliance on ISO standards, ISO/IEC

27004 is the correct and authoritative standard used to measure the effectiveness of an ISMS, making Option C the correct answer.

NEW QUESTION: 164

The executive board has requested that the CISO define Key Performance Indicators (KPIs) to measure the effectiveness of the security awareness program. Which information would be MOST useful?

- A.** Annual number of help desk tickets with the word "security" in them
- B.** Total number of employees that reported unsuccessful social engineering attacks
- C.** Month-by-month percentages of employees that failed phishing tests
- D.** Number of alerts detected by the Security Operations Center

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program defines KPIs as metrics that demonstrate performance trends and effectiveness over time. The most useful KPI for a security awareness program is month-by-month phishing failure rates, as this directly measures behavioral improvement.

CCISO materials emphasize that awareness effectiveness is best evaluated by reduced susceptibility to attacks, not activity volume. Help desk tickets (Option A) and SOC alerts (Option D) are indirect and noisy indicators. Reporting attempts (Option B) is useful but does not show failure trends.

Phishing test failure rates provide executives with a clear, trend-based performance indicator, making Option C correct.

NEW QUESTION: 165

Which of the following BEST mitigates ransomware threats?

- A. Phishing exercises
- B. Use immutable data storage
- C. Blocking use of wireless networks
- D. Application of multiple endpoint anti-malware solutions

Answer: ([SHOW ANSWER](#))

Immutable data storage is highly effective against ransomware threats because it ensures that stored data cannot be altered or deleted, even by malicious actors. This allows organizations to recover from ransomware attacks quickly without paying ransoms. Phishing exercises (A) and endpoint anti-malware (D) are preventive measures, while blocking wireless networks (C) is unrelated to ransomware mitigation.

NEW QUESTION: 166

The patching and monitoring of systems on a consistent schedule is required by?

- A. Local privacy laws
- B. Industry best practices
- C. Risk Management frameworks
- D. Audit best practices

Answer: ([SHOW ANSWER](#))

Patching and Monitoring as Best Practices:

Regular patching and system monitoring are considered best practices to ensure vulnerabilities are addressed promptly and systems remain secure.

Why This is Correct:

* Industry best practices emphasize consistency in patching and monitoring as foundational to maintaining a secure environment.

Why Other Options Are Incorrect:

* A. Local privacy laws: May require security but do not typically mandate patching schedules.

* C. Risk management frameworks: Focus on broader strategies, not specific operational practices.

* D. Audit best practices: Ensure compliance but don't define operational schedules.

References:

EC-Council aligns with industry best practices for patch management and system monitoring to maintain organizational security posture.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!
ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examd Discuss.com/EC-COUNCIL/exam/712-50/premium/> (**639** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 167

Ciphertext is encrypted with the same key used by the recipient to decrypt it. What encryption method is being used?

- A. Private key
- B. Key pairing
- C. Shared key
- D. Discrete key

Answer: C (LEAVE A REPLY)

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, when the same cryptographic key is used for both encryption and decryption, the encryption method is known as shared key encryption, also commonly referred to as symmetric key encryption.

In shared key encryption, both the sender and the recipient must possess the same secret key and ensure it is protected throughout its lifecycle. CCISO materials explain that symmetric encryption is computationally efficient and well-suited for encrypting large volumes of data, which is why it is widely used for data-at-rest and data-in-transit once a secure key exchange has occurred.

The term private key (Option A) is associated with asymmetric encryption, where a private key is paired with a public key. Key pairing (Option B) also refers to asymmetric cryptography, not shared-key methods.

Discrete key (Option D) is not a recognized cryptographic term within CCISO or industry standards.

CCISO emphasizes that while shared key encryption is efficient, it introduces key distribution and management risks, which must be addressed through secure key exchange mechanisms and governance controls.

Therefore, Option C: Shared key is the correct answer.

NEW QUESTION: 168

When analyzing and forecasting a capital expense budget what are not included?

- A. Network connectivity costs
- B. New datacenter to operate from

C. Upgrade of mainframe

D. Purchase of new mobile devices to improve operations

Answer: ([SHOW ANSWER](#))

When analyzing and forecasting a capital expense (CapEx) budget, network connectivity costs are not included as they are typically considered operating expenses (OpEx).

* Definition of CapEx:

* CapEx includes expenses for acquiring, upgrading, or building long-term assets like a new data center or equipment that will provide future benefits.

* Examples of CapEx:

* New datacenter: Classified as CapEx because it involves a significant upfront investment in long-term infrastructure.

* Mainframe upgrades: Involves significant costs for equipment upgrades, which are capitalized.

* New mobile devices: Asset purchase contributing to operational improvement, making it CapEx.

* Network Connectivity Costs:

* These are recurring expenses tied to maintaining internet and network services, categorized under OpEx.

* Financial Management in Security: Distinguishes between CapEx for infrastructure investment and OpEx for operational continuity.

NEW QUESTION: 169

Which of the following can the company implement in order to avoid this type of security issue in the future?

A. Network based intrusion detection systems

B. A security training program for developers

C. A risk management process

D. A audit management process

Answer: ([SHOW ANSWER](#))

* Security issues often arise due to vulnerabilities in the code. Training developers in secure coding practices helps mitigate this risk.

* A security training program equips developers to identify and address common vulnerabilities like injection flaws, insecure deserialization, and others.

Why Other Options Are Less Relevant:

* A. Network-based intrusion detection systems: Useful for detecting attacks but do not address the root cause of insecure coding.

* C. A risk management process: Focuses on organizational risk but does not directly resolve development flaws.

* D. An audit management process: Ensures compliance but does not directly enhance developer knowledge or secure coding practices.

EC-Council CISO Reference:

Emphasis is placed on proactive security measures, including developer training, as a core aspect of reducing vulnerabilities.

NEW QUESTION: 170

Human resource planning for security professionals in your organization is a:

- A. Simple and easy task because the threats are getting easier to find and correct.
- B. Training requirement that is met through once every year user training.
- C. Training requirement that is on-going and always changing.
- D. Not needed because automation and anti-virus software has eliminated the threats.

Answer: (SHOW ANSWER)

Dynamic Nature of Cybersecurity

- * Threat landscapes constantly evolve, requiring security professionals to undergo continuous training to stay updated on emerging risks, technologies, and best practices.
- * Annual training is insufficient for addressing real-time threats and vulnerabilities.

Comparison of Options

- * A. Simple and easy task: Incorrect, as cybersecurity threats are complex and evolving.
- * B. Once every year user training: User training alone does not cover the dynamic nature of cybersecurity threats.
- * D. Not needed due to automation: Incorrect, as human expertise remains critical despite automation tools.

EC-Council References

- * EC-Council highlights the need for continuous professional development and training as part of workforce development strategies for CISOs and their teams.

NEW QUESTION: 171

When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

- A. Vendors uses their own laptop and logins with same admin credentials your security team uses
- B. Vendor uses a company supplied laptop and logins using two factor authentication with same admin credentials your security team uses
- C. Vendor uses a company supplied laptop and logins using two factor authentication with their own unique credentials
- D. Vendor uses their own laptop and logins using two factor authentication with their own unique credentials

Answer: (SHOW ANSWER)

Best Practices for Vendor Access:

The EC-Council CISO framework emphasizes secure and controlled access for third-party vendors to reduce risks of unauthorized access, data breaches, or misuse.

Key Reasons for Option C:

- * Company-Supplied Laptop: Ensures compliance with internal security policies and avoids risks associated with unmanaged devices.

* Two-Factor Authentication (2FA): Adds an essential layer of security to prevent unauthorized access.

* Unique Credentials: Ensures accountability and enables tracking of vendor activities, reducing shared credential risks.

Why Not Other Options:

* Option A: Shared credentials create accountability issues and pose security risks.

* Option B: While 2FA is used, shared credentials are still a risk.

* Option D: Vendor's own laptop introduces risks from unverified device configurations.

EC-Council CISO Emphasis:

This approach aligns with best practices in third-party risk management, ensuring vendor access is secure, traceable, and compliant.

NEW QUESTION: 172

A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP).

In developing the business impact assessment (BIA), which of the following MOST closely relate to the data backup and restoral?

A. Recovery Point Objective (RPO)

B. Mean Time to Delivery (MTD)

C. Recovery Time Objective (RTO)

D. Maximum Tolerable Downtime (MTD)

Answer: ([SHOW ANSWER](#))

The Recovery Point Objective (RPO) represents the maximum acceptable amount of data loss measured in time before a disaster or disruption. RPO is critical for data backup and restoration in the Business Impact Assessment (BIA), as it determines the frequency of backups needed to meet continuity requirements. RTO (C) relates to the time required to recover systems, while MTD (D) defines the maximum downtime before critical impact.

Reference: <https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/#>:

~:text=The%20recovery%20time%20objective%20(RTO,consequences%20associated%20with%20the%20disruption

NEW QUESTION: 173

Which of the following is MOST useful when developing a business case for security initiatives?

A. Budget forecasts

B. Request for proposals

C. Cost/benefit analysis

D. Vendor management

Answer: ([SHOW ANSWER](#))

cost/benefit analysis evaluates the financial and operational advantages of a security initiative against its costs, helping build a strong business case.

* Foundation for Business Cases:

* Provides clarity on the financial return, operational improvements, and risk reductions offered by the initiative.

* Key Elements:

* Quantitative: Monetary costs and potential savings from risk mitigation.

* Qualitative: Non-financial benefits like improved reputation or compliance.

* Decision Support:

* Enables stakeholders to understand the trade-offs, ROI, and overall value, making it a cornerstone for justifying investments.

* Additional Factors:

* Budget forecasts, vendor proposals, and management considerations complement but do not replace a cost/benefit analysis.

* Strategic Justification: Outlines the importance of cost/benefit analysis in presenting security initiatives to decision-makers.

* Resource Allocation: Helps prioritize projects with maximum return and risk reduction.

NEW QUESTION: 174

You have implemented the new controls. What is the next step?

A. Document the process for the stakeholders

B. Monitor the effectiveness of the controls

C. Update the audit findings report

D. Perform a risk assessment

Answer: B ([LEAVE A REPLY](#))

Post-Implementation Step in Risk Management:

After implementing new controls, the next critical step is to monitor their effectiveness. This ensures the controls mitigate risks as intended and align with organizational goals.

Why Monitoring is Critical:

* Helps identify gaps or inefficiencies in the implemented controls.

* Provides data for further refinement or adjustment of the controls.

Why Other Options Are Incorrect:

* A. Document the process: Documentation follows monitoring for reporting accuracy.

* C. Update the audit findings report: Premature without confirming control effectiveness.

* D. Perform a risk assessment: Not the immediate step post-implementation.

References:

EC-Council emphasizes ongoing monitoring as essential for ensuring the sustained effectiveness of controls.

NEW QUESTION: 175

Which of the following illustrates an operational control?

- A. Conducting weekly audits of configuration management processes
- B. Establishing procurement guidelines for vendors
- C. Classifying an information system as part of a document assessment
- D. Installing a fire suppression system in a data center

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, operational controls are controls executed by people and processes as part of day-to-day operations to ensure security objectives are met.

Conducting weekly audits of configuration management processes is an example of an operational control because it involves recurring human-driven activities designed to maintain system integrity and compliance.

CCISO materials categorize controls into administrative (management), operational, technical, and physical.

Operational controls include procedures such as monitoring, reviews, audits, incident handling, and change verification-activities performed regularly to support security operations.

Establishing procurement guidelines (Option B) is an administrative/management control.

Classifying an information system (Option C) is a governance and documentation activity, also administrative. Installing a fire suppression system (Option D) is a physical control.

The CCISO program stresses that CISOs must ensure operational controls are effective because they directly influence how policies and standards are enforced in practice.

Therefore, Option A is correct.

NEW QUESTION: 176

An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in severe revenue disruptions.

Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

- A. The CISO
- B. Audit and Compliance
- C. The CFO
- D. The business owner

Answer: ([SHOW ANSWER](#))

Role of the Business Owner:

Business owners are responsible for operational processes and the associated risks. They are best positioned to evaluate the impact of disruptions and decide on risk acceptance.

Key Considerations:

- * Risk acceptance decisions should align with operational priorities and organizational objectives.
- * Business owners are directly accountable for revenue and operational outcomes.

Why Not Other Options:

- * CISO (A): Advises on security risks but does not own business process risks.

* Audit and Compliance (B): Monitors and validates adherence to controls but does not accept risk.

* CFO (C): Manages financial oversight but not specific operational risks.

EC-Council CISO Guidance:

Risk acceptance should reside with those closest to the operational impact, typically the business owner.

NEW QUESTION: 177

The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

- A. Defined metrics
- B. Operational metrics
- C. Audit metrics
- D. Management metrics

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation:

CCISO materials define operational metrics as measurements of day-to-day security activities and control performance. These metrics track effectiveness of operational processes such as patching, malware prevention, and vulnerability remediation.

NEW QUESTION: 178

An organization's Information Security Policy is of MOST importance because

- A. it communicates management's commitment to protecting information resources
- B. it is formally acknowledged by all employees and vendors
- C. it defines a process to meet compliance requirements
- D. it establishes a framework to protect confidential information

Answer: A (LEAVE A REPLY)

Purpose of an Information Security Policy:

- * The policy serves as a foundational document that articulates the organization's commitment to safeguarding its information assets.
- * It demonstrates management's intent and direction toward implementing robust security measures.

Management Commitment:

- * As per EC-Council CCISO, management's visible commitment to security is essential for creating a culture of compliance and accountability across the organization.
- * Policies provide a basis for decision-making, risk management, and incident response.

Supporting Reference:

- * The CCISO program outlines that a well-documented and communicated information security policy ensures clarity in roles and responsibilities, fostering alignment among all stakeholders, including employees and vendors.

NEW QUESTION: 179

How is an Annual Loss Expectancy (ALE) calculated?

- A. Single Loss Expectancy multiplied by the Annual Rate of Occurrence
- B. Total loss frequency multiplied by the total loss probability
- C. Replacement cost multiplied by the total loss expectancy
- D. Value of the asset multiplied by the lifecycle loss expectancy

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge defines Annual Loss Expectancy (ALE) as a quantitative risk metric calculated by multiplying Single Loss Expectancy (SLE) by the Annual Rate of Occurrence (ARO).

SLE represents the financial impact of a single incident, while ARO represents the expected frequency of occurrence per year. ALE provides a clear estimate of expected annual financial loss, enabling cost-benefit analysis and informed risk treatment decisions.

CCISO materials emphasize ALE as a foundational quantitative risk analysis tool used to justify security investments, compare mitigation options, and communicate risk in financial terms to executives.

Other formulas listed are not recognized CCISO risk equations. Therefore, the correct calculation is $SLE \times ARO$.

NEW QUESTION: 180

What is the BEST practice for having vendors verify controls within their services or products to protect customer data and systems?

- A. Validate controls once every five years
- B. Perform validations after contracts are signed
- C. Perform annual verifications
- D. Verify once during contract negotiations

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program emphasizes that ongoing assurance is critical for third-party risk management. The best practice is to require vendors to perform annual control verifications, such as SOC reports or compliance attestations.

One-time or infrequent validations (Options A and D) do not account for environmental, personnel, or system changes. Post-contract validation only (Option B) lacks continuous oversight. CCISO materials stress that annual verification aligns with audit cycles, regulatory expectations, and risk monitoring.

Therefore, Option C is correct.

NEW QUESTION: 181

Which type of physical security control scan a person's external features through a digital video camera before granting access to a restricted area?

- A. Retinal scan
- B. Iris scan
- C. Signature kinetics scan
- D. Facial recognition scan

Answer: ([SHOW ANSWER](#))

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam! ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (**639** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 182

Which of the following MOST heavily influences the information security governance model?

- A. Number of remote and on-site employees
- B. Audit management budgets
- C. Physical location of business units
- D. Organizational structures

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program identifies organizational structure as the dominant factor influencing the information security governance model.

CCISO documentation explains that governance determines authority, reporting lines, accountability, and decision-making, all of which are shaped by how the organization is structured (centralized, decentralized, matrixed). Workforce distribution, budgets, and geography influence operations but do not define governance authority.

Effective governance models must align with organizational design to ensure policies can be enforced and risks managed consistently.

Therefore, Option D is correct.

NEW QUESTION: 183

To make sure that the actions of all employees, applications, and systems follow the organization's rules and regulations can BEST be described as which of the following?

- A. Compliance management
- B. Asset management
- C. Risk management

D. Security management

Answer: ([SHOW ANSWER](#))

* Definition of Compliance Management:

* Involves ensuring that all employees, applications, and systems adhere to organizational rules, regulations, and legal requirements.

* Includes monitoring, enforcement, and reporting of compliance activities.

* Why Not Other Options:

* B: Asset management focuses on tracking and managing organizational assets.

* C: Risk management identifies and mitigates risks, not rule adherence.

* D: Security management pertains to safeguarding systems, not rule enforcement.

Reference:

EC-Council on Information Security Compliance Management

Reference: <https://www.eccouncil.org/information-security-management/>

NEW QUESTION: 184

As the CISO you need to write the IT security strategic plan. Which of the following is the MOST important to review before you start writing the plan?

A. The existing IT environment.

B. The company business plan.

C. The present IT budget.

D. Other corporate technology trends.

Answer: B ([LEAVE A REPLY](#))

Alignment with Business Objectives

* An IT security strategic plan must align with the company's overall business goals to ensure that security supports and enhances organizational objectives.

Why Review the Business Plan First

* Provides a clear understanding of organizational priorities, risks, and strategic directions.

* Helps identify critical assets and processes that require security investment.

Comparison of Options

* A. The existing IT environment: Important but secondary to aligning with business goals.

* C. The present IT budget: Helps in resource allocation but doesn't guide strategic alignment.

* D. Other corporate technology trends: Relevant but less critical than the business plan.

EC-Council References

* Strategic alignment is a core principle in EC-Council CISO guidance, ensuring security efforts support business resilience and growth.

NEW QUESTION: 185

A bastion host should be placed:

A. Inside the DMZ

B. In-line with the data center firewall

C. Beyond the outer perimeter firewall

D. As the gatekeeper to the organization's honeynet

Answer: C ([LEAVE A REPLY](#))

A bastion host is a fortified system designed to withstand attacks and is placed beyond the outer perimeter firewall to act as a buffer between the public network and internal systems. Its strategic location ensures it handles external-facing services securely, minimizing risks to internal networks. Placing it inside the DMZ (A) or inline with the data center firewall (B) limits its protective functionality. It is also distinct from honeynet management (D).

Reference: <https://www.skillset.com/questions/a-bastion-host-is-which-of-the-following>

NEW QUESTION: 186

Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

- A.** Single Loss Expectancy (SLE)
- B.** Exposure Factor (EF)
- C.** Annualized Rate of Occurrence (ARO)
- D.** Temporal Probability (TP)

Answer: ([SHOW ANSWER](#)**)**

Definition of ARO:

ARO estimates the frequency with which a specific threat is expected to occur in a year. It is a critical component of calculating Annual Loss Expectancy (ALE).

Why This is Correct:

ARO quantifies the likelihood of an event, allowing organizations to prioritize risk mitigation efforts effectively.

Why Other Options Are Incorrect:

- * A. SLE: Refers to the monetary loss from a single event.
- * B. EF: Represents the percentage of asset loss from a specific threat.
- * D. TP: Not a standard term in risk management frameworks.

References:

EC-Council highlights ARO as an essential metric for risk assessment and financial impact analysis in risk management frameworks.

NEW QUESTION: 187

What does the acronym RACI stand for?

- A.** Review, Act, Communicate, and Inform
- B.** Responsible, Accountable, Consulted, and Informed
- C.** Responsible, Authorized, Consulted, and Initiated
- D.** Researched, Advised, Communicated, and Implemented

Answer: ([SHOW ANSWER](#)**)**

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program defines RACI as a governance and accountability model standing for Responsible, Accountable, Consulted, and Informed. CCISO documentation

emphasizes that RACI matrices are critical for clarifying ownership, decision authority, and communication paths within security programs and enterprise initiatives.

"Responsible" identifies who performs the work, while "Accountable" designates the single individual ultimately answerable for outcomes. "Consulted" parties provide input or expertise, and "Informed" stakeholders are kept aware of progress or decisions. CCISO materials stress that proper use of RACI reduces confusion, eliminates duplicated effort, and strengthens executive oversight.

Other options either misrepresent governance terminology or omit accountability, which CCISO explicitly identifies as essential for security leadership. Therefore, Option B is correct.

NEW QUESTION: 188

What is the name of a formal statement that defines the strategy, approach, or expectations related to specific concerns within an organization:

- A. Procedure
- B. standard
- C. Guideline
- D. Policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 189

Which of the following refers to the quantity or quality of project deliverables expanding from the original project plan?

- A. Deliverable expansion
- B. Deadline extension
- C. Scope creep
- D. Scope modification

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 190

The Health Insurance Portability and Accountability Act (HIPAA) requires an agreement between Cloud Service Providers (CCSP) and the covered entity. Based on HIPAA, which document must be completed between the covered entity and the CCSP?

- A. Service Level Agreement (SLA)
- B. Memorandum of Understanding (MOU)
- C. Interconnection Security Agreement (ISA)
- D. Business Associate Agreement (BAA]

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 191

Which of the following is considered a project versus a managed process?

- A. monitoring external and internal environment during incident response

- B.** ongoing risk assessments of routine operations
- C.** continuous vulnerability assessment and vulnerability repair
- D.** installation of a new firewall system

Answer: ([SHOW ANSWER](#))

- * Projects are temporary endeavors undertaken to create a unique product, service, or result. Installing a new firewall is a one-time task with a defined start and end point, fitting the definition of a project.
- * Managed processes, on the other hand, are ongoing activities, such as monitoring or continuous risk assessment.

Why Other Options Are Incorrect:

- * A. Monitoring external and internal environments: This is a continuous process.
- * B. Ongoing risk assessments: By definition, ongoing activities are managed processes.
- * C. Continuous vulnerability assessment and repair: Ongoing by nature and therefore a process.

EC-Council CISO Reference:

Differentiating between projects and managed processes is crucial for resource allocation and management in security operations.

NEW QUESTION: 192

Scenario: Your company has many encrypted telecommunications links for their world-wide operations.

Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

How can you reduce the administrative burden of distributing symmetric keys for your employer?

- A.** Use asymmetric encryption for the automated distribution of the symmetric key
- B.** Use a self-generated key on both ends to eliminate the need for distribution
- C.** Use certificate authority to distribute private keys
- D.** Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

Answer: ([SHOW ANSWER](#))

Reducing the Burden of Key Distribution

- * Asymmetric encryption provides a secure mechanism for distributing symmetric keys without requiring physical transfer.
- * Public keys are used to encrypt the symmetric key, which can then be decrypted by the corresponding private key.

Why Not Other Options?

- * B. Use a self-generated key: Does not address distribution challenges.
- * C. Use a certificate authority: Distributes certificates, not symmetric keys.
- * D. Symmetrically encrypt and then decrypt: Adds unnecessary complexity without addressing distribution.

EC-Council References

- * Recommends hybrid encryption models that combine the strengths of symmetric and asymmetric encryption to streamline secure key distribution.

NEW QUESTION: 193

Physical security measures typically include which of the following components?

- A. Physical, Technical, Operational
- B. Technical, Strong Password, Operational
- C. Operational, Biometric, Physical
- D. Strong password, Biometric, Common Access Card

Answer: ([SHOW ANSWER](#))

* Physical security measures typically include:

* Physical: Locks, barriers, and surveillance systems.

* Technical: Access control systems and alarm systems.

* Operational: Security policies, procedures, and personnel training.

Why Other Options Are Incorrect:

* B. Technical, Strong Password, Operational: Passwords are part of logical security, not physical security.

* C. Operational, Biometric, Physical: Biometrics is part of technical security measures, not operational.

* D. Strong Password, Biometric, Common Access Card: Passwords are not physical security measures.

EC-Council CISO Reference:

The curriculum outlines the layered approach to security, with physical, technical, and operational components as critical for comprehensive protection.

NEW QUESTION: 194

What type of control is used when patching systems with the latest updates?

- A. Detection
- B. Dynamic blocking
- C. Zero day
- D. Corrective

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge classifies security controls into categories such as preventive, detective, corrective, and compensating. Patching systems with the latest updates is explicitly identified as a corrective control.

Corrective controls are implemented after a vulnerability or weakness has been identified, with the goal of remediating or correcting the issue to prevent further exploitation. CCISO materials explain that software vulnerabilities are often discovered after deployment, and patching is the primary mechanism used to correct these known weaknesses.

Detection controls, such as intrusion detection systems, only identify issues but do not fix them. Dynamic blocking is not a formal CCISO control category, and "zero day" refers to a type of vulnerability, not a control.

CCISO guidance further explains that effective patch management reduces attack surface, supports regulatory compliance, and demonstrates due diligence. While patching may also contribute to prevention, its primary classification remains corrective because it addresses existing vulnerabilities rather than stopping unknown threats in advance.

Thus, in alignment with CCISO control taxonomy, patching systems is a corrective control, making option D the correct answer.

NEW QUESTION: 195

When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it

- A.** In promiscuous mode and only detect malicious traffic.
- B.** In-line and turn on blocking mode to stop malicious traffic.
- C.** In promiscuous mode and block malicious traffic.
- D.** In-line and turn on alert mode to stop malicious traffic.

Answer: ([SHOW ANSWER](#))

Best Deployment Practice for IPS:

* Deploying an Intrusion Prevention System (IPS) in-line ensures that it can actively monitor and block malicious traffic as it flows through the network.

Blocking Malicious Traffic:

* Enabling blocking mode allows the IPS to act in real-time, preventing harmful actions rather than just alerting administrators.

Supporting Reference:

* CCISO materials highlight the importance of active threat prevention by deploying security systems in-line with blocking functionality enabled for maximum effectiveness.

NEW QUESTION: 196

What is a difference from the list below between quantitative and qualitative Risk Assessment?

- A.** Quantitative risk assessments result in an exact number (in monetary terms)
- B.** Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
- C.** Qualitative risk assessments map to business objectives
- D.** Quantitative risk assessments result in a qualitative assessment (high, medium, low, red, yellow, green)

Answer: ([SHOW ANSWER](#))

Difference Between Quantitative and Qualitative Assessments:

* Quantitative Assessment: Provides measurable data, often expressed in monetary terms, to quantify risk impact.

* Qualitative Assessment: Uses descriptive categories (e.g., high, medium, low) to assess risk based on subjective judgment.

Why Option A Is Correct:

Quantitative assessments focus on precise calculations, such as potential financial loss, which is a distinguishing feature.

Why Other Options Are Incorrect:

* B & D: These describe qualitative assessments, not quantitative.

* C. Mapping to Business Objectives: Both types can be mapped to objectives; this is not a distinguishing factor.

References:

EC-Council describes quantitative methods as data-driven and focused on objective metrics, while qualitative methods emphasize subjective risk prioritization.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!
ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 197

Which of the following is critical in creating a security program aligned with an organization's goals?

- A.** Ensure security budgets enable technical acquisition and resource allocation based on internal compliance requirements
- B.** Develop a culture in which users, managers and IT professionals all make good decisions about information risk
- C.** Provide clear communication of security program support requirements and audit schedules
- D.** Create security awareness programs that include clear definition of security program goals and charters

Answer: ([SHOW ANSWER](#))

Security Culture:

A strong security culture ensures that all organizational levels understand and prioritize security, leading to better decision-making about information risk.

Key Aspects:

- * Empowering users, managers, and IT professionals to understand and mitigate risks.
- * Encouraging proactive and informed participation in security processes.

Why Not Other Options:

* Budget management (A) and awareness programs (D) are supportive but not central to creating alignment.

* Communication of support requirements (C) is a tactical action, not a cultural shift.

EC-Council Emphasis:

A security-aware culture is fundamental to aligning security programs with organizational objectives.

NEW QUESTION: 198

Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

- A. Perform a vulnerability scan of the network
- B. External penetration testing by a qualified third party
- C. Internal Firewall ruleset reviews
- D. Implement network intrusion prevention systems

Answer: (SHOW ANSWER)

Why Penetration Testing is Effective:

- * Identifies weaknesses in perimeter defenses by simulating real-world attack scenarios.
- * Provides actionable insights for strengthening perimeter security.

Why This is Correct:

- * A qualified third party ensures unbiased testing and comprehensive evaluation.

Why Other Options Are Incorrect:

- * A. Vulnerability Scan: Identifies known vulnerabilities but lacks the depth of penetration testing.
- * C. Internal Firewall Reviews: Limited to rule analysis, not testing overall effectiveness.
- * D. Network Intrusion Prevention Systems: Mitigates threats but does not measure control effectiveness.

References:

EC-Council emphasizes external penetration testing as a critical tool for assessing perimeter network security controls.

NEW QUESTION: 199

Why is it vitally important that senior management endorse a security policy?

- A. So that they will accept ownership for security within the organization.
- B. So that employees will follow the policy directives.
- C. So that external bodies will recognize the organizations commitment to security.
- D. So that they can be held legally accountable.

Answer: (SHOW ANSWER)

Importance of Management Endorsement:

Senior management's endorsement of security policies ensures they take responsibility for integrating security into the organization's strategic objectives.

Ownership and Accountability:

- * Ensures that security policies are supported with adequate resources.

* Sets the tone for organizational culture, making security a priority across all levels.

Why Other Options Are Incorrect:

* B. Employee Adherence: Management support influences but is not directly tied to policy adherence.

* C. External Recognition: Endorsement is for internal accountability, not external validation.

* D. Legal Accountability: While management may bear some responsibility, this is not the primary reason for endorsement.

References:

EC-Council emphasizes the critical role of senior management in establishing ownership and fostering a security-driven culture.

NEW QUESTION: 200

Ciphertext is encrypted with a result being a compressed representation of the original data. What is this result called?

A. Shared key

B. Multi-factor

C. Ciphertext

D. One-time hash

Answer: D ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, a one-way hash (often referred to as a one-time hash) is a compressed, fixed-length representation of original data produced by a hashing algorithm.

Hashing differs from encryption in that it is non-reversible. The original data cannot be reconstructed from the hash value. CCISO materials explain that hashes are commonly used for integrity verification, password storage, and digital signatures.

Shared key (Option A) and multi-factor (Option B) are unrelated to data representation. Ciphertext (Option C) refers to encrypted data that can be decrypted, unlike a hash.

Therefore, Option D is correct.

NEW QUESTION: 201

When gathering security requirements for an enterprise software solution, which of the following is MOST important?

A. Type of encryption provided for data at rest

B. Type of data contained in the system and how it is used

C. Type of connection and protocol used to transfer configuration information

D. Brand of platform the application is hosted on

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, understanding the type of data and its business use is the most critical factor when defining security requirements.

CCISO materials emphasize data-driven security, where classification, sensitivity, regulatory impact, and usage dictate encryption, access controls, monitoring, and retention. Encryption, protocols, and platforms (Options A, C, and D) are secondary implementation decisions derived from data risk.

Therefore, Option B is correct.

NEW QUESTION: 202

Which of the following best summarizes the primary goal of a security program?

- A. Provide security reporting to all levels of an organization
- B. Create effective security awareness to employees
- C. Manage risk within the organization
- D. Assure regulatory compliance

Answer: ([SHOW ANSWER](#))

Primary Goal of a Security Program:

The overarching goal of a security program is to manage risks to the organization's assets, operations, and reputation. By identifying, assessing, and mitigating risks, a security program ensures operational continuity and safeguards critical information.

Key Considerations:

- * Risk management is central to aligning security objectives with business goals.
- * While regulatory compliance (D), reporting (A), and awareness (B) are components of a security program, they serve the broader purpose of risk management.

EC-Council CISO Guidance:

Risk management is emphasized as the cornerstone of an effective security program, aligning with the organization's strategy and objectives.

NEW QUESTION: 203

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

- A. Setup a mock video camera next to the special card reader adjacent to the secure door
- B. Educate and enforce physical security policies of the company to all the employees on a regular basis
- C. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door
- D. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 204

Risk that remains after risk mitigation is known as

- A. Persistent risk
- B. Residual risk
- C. Accepted risk
- D. Non-tolerated risk

Answer: ([SHOW ANSWER](#))

Definition of Residual Risk:

* Residual risk refers to the risk remaining after implementing risk mitigation measures.

Managing Residual Risk:

* It is the responsibility of security executives to assess and accept residual risks based on the organization's risk tolerance and appetite.

Supporting Reference:

* The CCISO program highlights residual risk management as a critical part of risk management frameworks, emphasizing continuous monitoring.

NEW QUESTION: 205

The primary responsibility for assigning entitlements to a network share lies with which role?

- A. CISO
- B. Data owner
- C. Chief Information Officer (CIO)
- D. Security system administrator

Answer: ([SHOW ANSWER](#))

* Role of Data Owner:

* The data owner is responsible for defining and assigning entitlements to access network shares or other data repositories.

* They establish permissions based on business needs and sensitivity of the data.

* Why Not Other Options:

* A: The CISO sets security policies but does not manage specific entitlements.

* C: The CIO oversees IT strategy but typically delegates entitlement assignments to data owners.

* D: Security system administrators implement permissions but do not define them.

Reference:

Infosec Institute on Data Ownership and Entitlement Assignment

Reference: <https://resources.infosecinstitute.com/certification/data-and-system-ownership/>

NEW QUESTION: 206

What is protected by Federal Information Processing Standards (FIPS) 140-2?

- A. Confidentiality
- B. Non-repudiation
- C. Availability
- D. Integrity

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 207

Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

- A.** To give information security management recommendations to those who are responsible for initiating, implementing, or maintaining security in their organization.
- B.** To provide a common basis for developing organizational security standards
- C.** To provide effective security management practice and to provide confidence in inter-organizational dealings
- D.** To established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization

Answer: ([SHOW ANSWER](#))

Purpose of ISO 27002:

ISO 27002 provides detailed guidance for implementing the controls outlined in ISO 27001, catering to security professionals managing organizational security.

Why This is Correct:

- * Focuses on actionable recommendations for security implementation and management.

Why Other Options Are Incorrect:

- * B. Common basis for standards: A broader goal, not the primary purpose.
- * C. Effective security management practice: A benefit, not the main objective.
- * D. Guidelines and general principles: Overlaps with ISO 27001, not ISO 27002.

References:

EC-Council aligns ISO 27002 with practical recommendations for managing and maintaining information security systems.

NEW QUESTION: 208

SCENARIO: Critical servers show signs of erratic behavior within your organization's intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.

During initial investigation, the team suspects criminal activity but cannot initially prove or disprove illegal actions. What is the MOST critical aspect of the team's activities?

- A.** Regular communication of incident status to executives
- B.** Eradication of malware and system restoration
- C.** Determination of the attack source
- D.** Preservation of information

Answer: ([SHOW ANSWER](#))

During an investigation where criminal activity is suspected, preservation of information is critical to ensure evidence is not altered or destroyed, maintaining its integrity for potential legal proceedings.

* Key Considerations in Criminal Investigations:

* Maintain chain of custody to ensure admissibility of evidence.

* Document and preserve logs, artifacts, and affected system states.

* Other Activities:

* Communication: Important but secondary to preserving evidence.

* Eradication and Restoration: Typically done after evidence is collected.

* Determining Attack Source: Valuable but dependent on preserved data.

* Incident Handling and Forensics: Stresses the importance of evidence preservation in investigations.

* Legal and Compliance Requirements: Aligns with the need for defensible evidence in cases of suspected criminal activity.

NEW QUESTION: 209

When developing the Business Impact Assessment (BIA), which of the following MOST closely relates to data backup and restoration?

A. Mean Time to Del very >MTD)

B. Recovery Time Objective (RTO)

C. Recovery Point Objective (RPO)

D. Maximum Tolerable Downtime (MTD)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 210

Which of the following metrics would be MOST effective for measuring the effectiveness of a newly implemented change control process?

A. Total unrequested changes

B. Unplanned system outage trends

C. Duration of planned outages

D. Monthly count of rejected change requests

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The CCISO framework identifies reduction in unplanned outages as the most effective indicator of a successful change control process. CCISO materials emphasize outcome-based metrics over activity-based metrics.

Unplanned outages directly reflect whether changes are properly reviewed, tested, and approved. Other metrics measure volume or efficiency but do not clearly demonstrate effectiveness.

NEW QUESTION: 211

What is an approach to estimating the strengths and weaknesses of alternatives used to determine options, which provide the BEST approach to achieving benefits while preserving savings called?

- A. Business Impact Analysis
- B. Economic Impact analysis
- C. Return on Investment
- D. Cost-benefit analysis

Answer: D (LEAVE A REPLY)

Cost-benefit analysis (CBA) is a method used to evaluate the strengths and weaknesses of alternatives to determine the most cost-effective way to achieve benefits while preserving savings. This involves comparing the expected costs and benefits of a decision, ensuring optimal allocation of resources. It is more specific to decision-making than Business Impact Analysis (A), Economic Impact Analysis (B), or Return on Investment (C), which focus on other financial or strategic aspects.

Reference: <https://artsandculture.google.com/entity/cost%E2%80%93benefit-analysis/m020w0x?hl=en>

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam! ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdisscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 212

Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

- A. Define the risk appetite
- B. Determine budget constraints
- C. Review project charters
- D. Collaborate security projects

Answer: (SHOW ANSWER)

- * Defining risk appetite provides clear guidance on how much risk is acceptable, helping balance innovation with caution.
- * It ensures that decisions around innovation and security align with the organization's overall risk tolerance.

Why Other Options Are Less Effective:

- * B. Determine budget constraints: Budget constraints are important but do not address the balance between innovation and caution.

- * C. Review project charters: Reviewing charters provides project-specific insights but does not address organizational risk strategy.
- * D. Collaborate security projects: Collaboration is helpful but not as foundational as defining risk appetite.

EC-Council CISO Reference:

Understanding and articulating risk appetite is a core component of governance and strategic alignment in the CISO program.

NEW QUESTION: 213

When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

- A. Type of encryption required for the data once it is at rest
- B. Type of connection/protocol used to transfer the data
- C. Type of computer the data is processed on
- D. Type of data contained in the process/system

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 214

A security project is over a year behind schedule and over budget. Which of the following is MOST important to review and verify?

- A. Constraints
- B. Scope
- C. Technologies
- D. Milestones

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program emphasizes that scope management is the single most critical factor affecting project schedule and budget performance. When a security project is significantly delayed and over budget, CCISO documentation identifies scope creep or poorly defined scope as the most common root cause.

Scope defines what is included and excluded in the project. If scope is not properly defined, controlled, and approved, additional requirements are often introduced without corresponding adjustments to budget, schedule, or resources. CCISO training explicitly states that unresolved scope issues frequently manifest as missed milestones, cost overruns, and stakeholder dissatisfaction.

Constraints (Option A) such as time, cost, and resources are outcomes affected by scope, not the primary driver. Technologies (Option C) may contribute to complexity, but technology challenges are typically symptoms of scope expansion or unclear requirements. Milestones (Option D) are tracking mechanisms; reviewing milestones alone does not address the root cause of project failure.

CCISO governance guidance aligns with PMI and ISO project governance principles, reinforcing that CISOs must verify scope first when projects fail, before addressing execution details. Proper scope review allows leadership to determine whether the project remains viable, needs re-baselining, or requires executive intervention.

Therefore, the most important element to review and verify is the project scope, making Option B the correct answer.

NEW QUESTION: 215

During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

- A.** Identify and evaluate the existing controls.
- B.** Disclose the threats and impacts to management.
- C.** Identify information assets and the underlying systems.
- D.** Identify and assess the risk assessment process used by management.

Answer: ([SHOW ANSWER](#))

Risk Analysis Process:

* After identifying threats and impacts, the next logical step is to assess existing controls to determine their effectiveness in mitigating identified risks.

Why This is Correct:

* Evaluating controls helps identify gaps or weaknesses requiring further mitigation.

Why Other Options Are Incorrect:

- * B. Disclosing to management: Premature before evaluating controls.
- * C. Identify information assets: Should occur earlier in the risk analysis.
- * D. Assessing risk processes: A broader task, not specific to this step.

References:

EC-Council highlights the importance of evaluating existing controls as part of the risk management process to determine residual risks.

NEW QUESTION: 216

The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

- A.** Fence
- B.** Video surveillance
- C.** Mantrap
- D.** Bollards

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 217

As the CISO for your company you are accountable for the protection of information resources commensurate with:

- A. Customer demand
- B. Cost and time to replace
- C. Insurability tables
- D. Risk of exposure

Answer: ([SHOW ANSWER](#))

CISO Accountability:

* As a CISO, your primary accountability is to ensure the protection of information resources based on the risk of exposure to potential threats.

* This involves assessing the likelihood and impact of risks, implementing appropriate safeguards, and ensuring resources are adequately protected relative to their value and potential impact.

Why Other Options Are Incorrect:

* A. Customer demand: While customer satisfaction is critical, it is not the primary measure of protection.

* B. Cost and time to replace: This is a factor in risk analysis but not the sole determinant of protection strategies.

* C. Insurability tables: Insurance metrics may inform risk decisions but do not define overall accountability.

EC-Council CISO Reference:

The curriculum emphasizes the importance of risk management and aligning security measures with the organization's risk tolerance and potential exposure.

NEW QUESTION: 218

Over 90% of successful cyber-attacks currently include: Social engineering

- A. Social engineering
- B. Phishing Attacks
- C. Misconfiguration
- D. All of these

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 219

Where does bottom-up financial planning primarily gain information for creating budgets?

- A. By adding the cost of all known individual tasks and projects that are planned for the next budgetary cycle
- B. By adding all capital and operational costs from the prior budgetary cycle, and determining potential financial shortages
- C. By reviewing last year's program-level costs and adding a percentage of expected additional portfolio costs
- D. By adding all planned operational expenses per quarter then summarizing them in a budget request

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 220

A stakeholder is a person or group:

- A. Vested in the success and/or failure of a project or initiative regardless of budget implications.
- B. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
- C. That has budget authority.
- D. That will ultimately use the system.

Answer: ([SHOW ANSWER](#))

Definition of a Stakeholder:

* Stakeholders include anyone with an interest in the success or failure of a project or initiative, irrespective of their direct financial involvement or usage of the system.

Why Other Options Are Incorrect:

- * B. Vested in success and tied to budget: Budget involvement is not a prerequisite for being a stakeholder.
- * C. That has budget authority: Stakeholders are not limited to those with financial control.
- * D. That will ultimately use the system: Users are stakeholders, but stakeholders are not limited to end- users.

EC-Council CISO Reference:

EC-Council defines stakeholders broadly to include all parties affected by or invested in a project's outcome, emphasizing their influence and varied roles.

NEW QUESTION: 221

Which security technologies are critical for a zero trust model?

- A. Multi-factor authentication, Identity and Access Management (IAM), and endpoint security
- B. Coding libraries, secure network gateways, and endpoint antivirus
- C. Data Loss Prevention (DLP), Security Information and Event Management (SIEM), and network integrations
- D. Firewalls, intrusion prevention, and Web Application Firewalls (WAF)

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

The EC-Council CCISO program aligns zero trust architecture with the principle of "never trust, always verify." CCISO documentation emphasizes that zero trust is identity-centric, not perimeter-centric, making multi-factor authentication (MFA), identity and access management (IAM), and endpoint security the most critical enabling technologies.

MFA ensures that access decisions are not based on a single factor such as a password. IAM enforces least privilege, continuous authentication, and access policy enforcement. Endpoint security validates device posture, health, and trustworthiness before granting access. Together, these controls enable continuous verification of users, devices, and sessions, which is the foundation of zero trust.

Firewalls, IPS, WAFs, SIEM, and DLP (Options C and D) are important supporting controls but do not define zero trust. CCISO materials explicitly state that zero trust shifts security decisions away from network location and toward identity, context, and device trust.

Therefore, Option A is correct.

NEW QUESTION: 222

Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

- A. It allows executives to more effectively monitor IT implementation costs
- B. Implementation of it eases an organization's auditing and compliance burden
- C. Information Security (IS) procedures often require augmentation with other standards
- D. It provides for a consistent and repeatable staffing model for technology organizations

Answer: ([SHOW ANSWER](#))

COBIT Overview:

COBIT (Control Objectives for Information and Related Technology) provides a comprehensive framework for managing and governing IT. It focuses on aligning IT operations with organizational goals, streamlining audit readiness, and supporting regulatory compliance.

Auditing and Compliance Burden:

COBIT includes control objectives and guidelines that map directly to compliance requirements (e.g., SOX, GDPR). EC-Council CISO highlights the importance of frameworks like COBIT in reducing compliance complexity and ensuring consistent implementation of controls.

Why COBIT Is the Best Choice:

- * It ensures alignment between IT objectives and business goals.
- * Facilitates efficient internal and external audits by standardizing processes.
- * Reduces redundant work by integrating compliance and operational controls.

Alignment with EC-Council CISO Principles:

This option aligns with the EC-Council CISO's focus on efficiency and risk-based compliance management.

NEW QUESTION: 223

The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees.

Which of the following can be used as a KPI?

- A. Number of callers who report security issues.
- B. Number of callers who report a lack of customer service from the call center
- C. Number of successful social engineering attempts on the call center
- D. Number of callers who abandon the call before speaking with a representative

Answer: ([SHOW ANSWER](#))

Purpose of KPIs in Security Awareness Programs:

- * KPIs measure the effectiveness of training programs in preventing security incidents like social engineering attacks.

* Tracking the success rate of social engineering attempts provides actionable insights into program effectiveness.

Why This is Correct:

* Directly measures the effectiveness of employees in identifying and resisting social engineering attempts.

Why Other Options Are Incorrect:

* A. Number of callers reporting security issues: Indicates reporting but not program effectiveness.

* B. Lack of customer service: Unrelated to security awareness.

* D. Call abandonment rate: Operational metric, not a security KPI.

References:

EC-Council emphasizes KPIs that directly measure the outcomes of security awareness training programs.

NEW QUESTION: 224

The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

A. Organization control

B. Procedural control

C. Management control

D. Technical control

Answer: ([SHOW ANSWER](#))

Anti-Malware and Anti-Phishing Controls:

* These are technical controls as they involve the use of technology to detect and mitigate malware and phishing threats.

Application Context:

* Centralized email server protections are technical implementations to secure communication channels.

Supporting Reference:

* CCISO materials categorize anti-malware and anti-phishing measures as technical controls essential for defending against cyber threats.

NEW QUESTION: 225

When you develop your audit remediation plan what is the MOST important criteria?

A. To validate that the cost of the remediation is less than the risk of the finding.

B. To validate the remediation process with the auditor.

C. To remediate half of the findings before the next audit.

D. To remediate all of the findings before the next audit.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 226

A security project gets a great deal of resistance across the organization. Which of the following represents the MOST likely reason for this situation?

- A. The project is no longer required for securing the organization
- B. The organization was not properly trained on security and privacy requirements
- C. Software licenses were out of synchronization with other systems
- D. The project was initiated without support from the affected business units

Answer: D (LEAVE A REPLY)

Comprehensive and Detailed Explanation:

CCISO leadership guidance consistently identifies lack of business-unit buy-in as the most common reason for resistance to security initiatives. Projects initiated without stakeholder involvement often conflict with operational needs, resulting in pushback and failure.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam! ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdisscuss.com/EC-COUNCIL/exam/712-50/premium/> (**639** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 227

What is a key policy that should be part of the information security plan?

- A. Account management policy
- B. Training policy
- C. Acceptable Use policy
- D. Remote Access policy

Answer: (SHOW ANSWER)

An Acceptable Use Policy (AUP) is a critical component of an information security plan, as it defines acceptable and unacceptable actions for system and resource usage. It ensures users understand their responsibilities, reducing risks from misuse or negligence. While account management (A), training (B), and remote access (D) policies are important, the AUP provides the broad foundational guidance for user behavior.

Reference: <https://www.exabeam.com/information-security/information-security-policy/>

NEW QUESTION: 228

Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.

You have identified potential solutions for all of your risks that do not have security controls. What is the NEXT step?

- A. Get approval from the board of directors
- B. Screen potential vendor solutions
- C. Verify that the cost of mitigation is less than the risk
- D. Create a risk metrics for all unmitigated risks

Answer: ([SHOW ANSWER](#))

The next step after identifying potential solutions is to verify that the cost of mitigation is less than the risk.

This ensures that mitigation strategies are cost-effective and align with the organization's risk appetite.

* Cost-Risk Analysis:

- * Assess the financial and operational impact of proposed controls.
- * Ensure the cost of implementing controls is justified by the reduction in risk.

* Sequence of Actions:

- * Only after verifying cost-effectiveness should the board of directors or vendors be engaged.
- * Risk metrics and vendor screening are subsequent activities based on selected solutions.

* Risk-Based Decision Making:

- * Decisions prioritize solutions that provide optimal security without exceeding the value of the protected asset.

* Cost-Benefit Analysis in Risk Management: Emphasizes evaluating cost-effectiveness as a critical step in risk mitigation.

* Strategic Risk Reduction: Aligns mitigation efforts with organizational risk tolerances.

NEW QUESTION: 229

What Enterprise Architecture Framework is business-centric and is composed of eight phases?

- A. Sherwood Applied Business Security Architecture
- B. Federal Enterprise Architecture
- C. Zochman
- D. The Open Group Architecture Framework (TOGAF)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 230

A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

- A. Providing a risk program governance structure
- B. Ensuring developers include risk control comments in code
- C. Creating risk assessment templates based on specific threats
- D. Allowing for the acceptance of risk for regulatory compliance requirements

Answer: ([SHOW ANSWER](#))

Importance of Governance Structure in Risk Programs:

Governance provides the framework for accountability, decision-making, and alignment with organizational objectives. A governance structure ensures that the risk program is effectively managed and integrated into the organization's operations.

Critical Elements of Governance:

- * Establishing clear roles and responsibilities.
- * Defining reporting mechanisms and oversight.
- * Ensuring alignment with business and regulatory requirements.

Why Other Options Are Incorrect:

- * B. Developers Including Risk Control Comments: This is specific to coding practices, not program governance.
- * C. Risk Assessment Templates: Helpful but not the primary driver for program success.
- * D. Accepting Risk for Compliance: A tactical approach, not a strategic governance aspect.

References:

EC-Council emphasizes the significance of governance in ensuring the success and sustainability of risk management programs.

NEW QUESTION: 231

The single most important consideration to make when developing your security program, policies, and processes is:

- A. Budgeting for unforeseen data compromises
- B. Streamlining for efficiency
- C. Alignment with the business
- D. Establishing your authority as the Security Executive

Answer: C ([LEAVE A REPLY](#))

Importance of Alignment with Business Objectives:

- * According to the EC-Council CCISO framework, aligning the security program with business objectives ensures that security measures support the organization's strategic goals.
- * This alignment is critical to gaining executive buy-in and justifying the investment in security measures.

Business-Driven Security Approach:

- * The CCISO program emphasizes that a security strategy disconnected from business goals can lead to inefficiencies, reduced support from leadership, and inadequate protection.
- * Security should not be a standalone function but integrated into business processes to maximize its effectiveness.

Supporting Reference:

- * EC-Council training material highlights alignment with business objectives as the cornerstone of governance, risk management, and compliance (GRC) practices. This approach ensures that security enhances business resilience while minimizing risk.

NEW QUESTION: 232

Which of the following terms is defined as the friction or opposition resulting from actual or perceived differences or incompatibilities?

- A. Agreement
- B. Silos
- C. Disgruntlement
- D. Conflict

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

Within the EC-Council CCISO leadership and governance modules, the term conflict is explicitly defined as the friction or opposition arising from actual or perceived differences, incompatibilities, or competing interests. CCISO materials stress that conflict is a natural and unavoidable element of organizational dynamics, particularly in complex environments involving business units, IT, security teams, and executive leadership.

CCISO training highlights that conflicts frequently arise due to differing priorities-such as security versus usability, cost versus risk reduction, or operational speed versus control enforcement.

Recognizing and managing conflict effectively is a critical leadership responsibility for CISOs, as unresolved conflict can undermine governance, weaken security programs, and reduce organizational trust.

Other options do not align with the CCISO definition. Agreement represents alignment rather than opposition.

Silos describe organizational separation but do not inherently imply friction. Disgruntlement reflects dissatisfaction but does not fully capture the interaction-based opposition implied in the definition of conflict.

The CCISO program emphasizes that effective conflict management strengthens collaboration, improves decision-making, and enables security leaders to align security objectives with business goals. CISOs must apply communication, negotiation, and influence skills to resolve conflicts constructively.

Therefore, according to CCISO terminology and leadership principles, conflict is the correct and verified answer.

NEW QUESTION: 233

Which of the following are the MOST important factors for proactively determining system vulnerabilities?

- A. Subscribe to vendor mailing list to get notification of system vulnerabilities
- B. Deploy Intrusion Detection System (IDS) and install anti-virus on systems
- C. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
- D. Conduct security testing, vulnerability scanning, and penetration testing

Answer: (SHOW ANSWER)

Proactive Vulnerability Identification:

* Security testing, vulnerability scanning, and penetration testing are essential for uncovering and addressing weaknesses before they are exploited.

Comprehensive Approach:

* These activities provide detailed insights into the security posture and help prioritize remediation efforts.

Supporting Reference:

* CCISO stresses regular and thorough security assessments as a cornerstone of proactive vulnerability management.

NEW QUESTION: 234

An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?

- A. Determine the risk tolerance
- B. Perform an asset classification
- C. Create an architecture gap analysis
- D. Analyze existing controls on systems

Answer: ([SHOW ANSWER](#))

Next Step After Defining Controls:

* After setting security standards and conditions, the logical progression is to analyze existing controls to identify gaps or redundancies in the current systems.

Rationale:

* This analysis provides insight into whether existing controls align with defined standards and identifies areas requiring improvement.

Supporting Reference:

* The CCISO framework emphasizes control analysis as a key step in implementing an effective security program and achieving compliance with security standards.

NEW QUESTION: 235

You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll. Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff? (choose the best answer):

- A. Deploy a SEIM solution and have current staff review incidents first thing in the morning
- B. Contract with a managed security provider and have current staff on recall for incident response
- C. Configure your syslog to send SMS messages to current staff when target events are triggered
- D. Employ an assumption of breach protocol and defend only essential information resources

Answer: ([SHOW ANSWER](#))

* Explanation:

- * Contracting with a managed security service provider (MSSP) offers 24/7 monitoring and incident detection capabilities without adding full-time staff.
- * Current staff can remain on-call for critical incident response, ensuring coverage without increasing headcount.
- * Why Other Options Are Incorrect:
 - * A. Deploy a SEIM solution: While useful, a SEIM requires constant monitoring to be effective. Simply reviewing incidents in the morning is insufficient.
 - * C. Configure syslog to send SMS messages: This approach lacks comprehensive monitoring and is reactive rather than proactive.
 - * D. Employ an assumption of breach protocol: This does not address the need for consistent monitoring and is not a direct solution to coverage gaps.
- * EC-Council CISO Reference: The program highlights the value of MSSPs in enhancing organizational security capabilities while managing costs.

NEW QUESTION: 236

SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs.

What is the MOST logical course of action the CISO should take?

- A.** Review the original solution set to determine if another system would fit the organization's risk appetite and budget/regulatory compliance requirements
- B.** Continue with the implementation and submit change requests to the vendor in order to ensure required functionality will be provided when needed
- C.** Continue with the project until the scalability issue is validated by others, such as an auditor or third party assessor
- D.** Cancel the project if the business need was based on internal requirements versus regulatory compliance requirements

Answer: (SHOW ANSWER)

When discovering that a selected solution no longer meets the organization's scalability needs, the most logical course of action is to review the original solution set to find an alternative that aligns with the organization's risk appetite, budget, and compliance requirements.

- * Issue Identification:
 - * Scalability issues mean the solution is not fit for purpose.
 - * Proceeding with the implementation risks wasting resources and failing to meet organizational needs.
- * Best Approach:
 - * Reassess the available options from the original evaluation.
 - * Ensure the alternative solution meets both functional and regulatory requirements.
- * Other Options:

- * B & C: Continuing the implementation with unresolved scalability issues could lead to operational failures.
- * D: Canceling the project based solely on internal requirements disregards the broader business context.
- * Risk-Based Decision Making: Encourages reassessing alternatives when new risks are identified.
- * Project Management Principles: Stresses alignment of solutions with business needs and compliance requirements.

NEW QUESTION: 237

XYZ is a publicly-traded software development company.

Who is ultimately accountable to the shareholders in the event of a cybersecurity breach?

- A. Chief Financial Officer (CFO)
- B. Chief Software Architect (CIO)
- C. CISO
- D. Chief Executive Officer (CEO)

Answer: D (LEAVE A REPLY)

- * CEO Accountability:
- * As the highest-ranking executive, the CEO is ultimately accountable to shareholders for all organizational risks, including cybersecurity breaches.
- * This accountability stems from their responsibility for overall strategy, performance, and risk management.
- * Why Not Other Options:
- * A: The CFO manages financial risks, not cybersecurity accountability.
- * B: The CIO oversees technology but is not directly accountable to shareholders.
- * C: The CISO manages cybersecurity but reports to the CEO or equivalent.

Reference:

EC-Council on Executive Roles and Shareholder Accountability in Security Management

Reference: <https://www.eccouncil.org/information-security-management/>

NEW QUESTION: 238

What is meant by password aging?

- A. An expiration date set for passwords
- B. A Single Sign-On requirement
- C. Time in seconds a user is allocated to change a password
- D. The amount of time it takes for a password to activate

Answer: (SHOW ANSWER)

- * Password Aging Concept:
- * Password aging involves setting a maximum duration a password remains valid, after which the user must change it.
- * This approach helps mitigate risks of compromised passwords being exploited indefinitely.

- * Implementation Details:
- * Policies typically enforce expiration periods (e.g., 30, 60, or 90 days).
- * Notifications are sent to users prior to expiration to ensure timely updates.
- * Benefits:
- * Enhances security by limiting exposure to compromised credentials.
- * Aligns with compliance requirements (e.g., PCI DSS, ISO 27001).

Reference:

Medical Dictionary Definition of Password Aging: Password expiration is a fundamental security policy for ensuring account security.

Reference: <https://medical-dictionary.thefreedictionary.com/password+ageing>

NEW QUESTION: 239

Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?

- A. Terms and Conditions
- B. Service Level Agreements (SLA)
- C. Statement of Work
- D. Key Performance Indicators (KPI)

Answer: (SHOW ANSWER)

Role of SLAs in Contractual Obligations:

Service Level Agreements define specific performance metrics and obligations that vendors must meet, ensuring alignment with customer expectations.

Key Features of SLAs:

- * Clearly outlines deliverables, response times, and performance standards.
- * Includes penalties or corrective measures for non-compliance.

Why Not Other Options:

- * Terms and Conditions (A): Provide general legal guidelines but lack detailed performance metrics.
- * Statement of Work (C): Describes tasks but does not enforce performance levels.
- * Key Performance Indicators (D): Metrics for monitoring but not binding contractual terms.

EC-Council Guidance:

SLAs ensure accountability and clarity in vendor-customer relationships, aligning with CISO best practices for vendor management.

NEW QUESTION: 240

Dataflow diagrams are used by IT auditors to:

- A. Order data hierarchically.
- B. Highlight high-level data definitions.
- C. Graphically summarize data paths and storage processes.
- D. Portray step-by-step details of data generation.

Answer: C (LEAVE A REPLY)

Purpose of Dataflow Diagrams:

- * Visual representation of how data moves through a system, including paths, processes, and storage locations.

Why This is Correct:

- * Provides auditors with an overview of system processes and data handling practices.
- * Helps identify vulnerabilities or inefficiencies in data handling.

Why Other Options Are Incorrect:

- * A. Order data hierarchically: Not the function of dataflow diagrams.
- * B. Highlight high-level data definitions: Focuses on detail, not flow.
- * D. Step-by-step details: Refers to process flows, not dataflows.

References:

Dataflow diagrams are a standard tool referenced by EC-Council for mapping data handling processes during audits.

NEW QUESTION: 241

A global retail company is creating a new compliance management process. Which of the following regulations is of MOST importance to be tracked and managed by this process?

- A. Information Technology Infrastructure Library (ITIL)
- B. International Organization for Standardization (ISO) standards
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. National Institute for Standards and Technology (NIST) standard

Answer: (SHOW ANSWER)

Importance of PCI-DSS for Retail Companies:

- * Retail businesses frequently handle payment card transactions, making PCI-DSS compliance essential for securing cardholder data.
- * Non-compliance with PCI-DSS can lead to severe financial penalties and reputational damage.

Why PCI-DSS is Prioritized:

- * Directly addresses the protection of sensitive payment data.
- * Specifically relevant to the retail sector.

Why Other Options Are Incorrect:

- * A. ITIL: Focuses on IT service management, not retail compliance.
- * B. ISO Standards: General guidelines, not specific to payment card data.
- * D. NIST Standards: Primarily for federal agencies and not tailored for retail compliance.

References:

EC-Council emphasizes PCI-DSS as the critical standard for organizations handling payment data, especially in retail.

exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 242

Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network.

Which is the single most important factor to introducing digital evidence into a court of law?

- A. Comprehensive Log-Files from all servers and network devices affected during the attack
- B. Fully trained network forensic experts to analyze all data right after the attack
- C. Uninterrupted Chain of Custody
- D. Expert forensics witness

Answer: (SHOW ANSWER)

* Chain of custody refers to the documentation and handling process that ensures digital evidence is collected, preserved, and transferred without tampering.

* It is the most critical factor for legal admissibility, ensuring the integrity of the evidence from collection to courtroom presentation.

Why Other Options Are Incorrect:

- * A. Comprehensive log files: Logs are vital but meaningless in court without a proven chain of custody.
- * B. Trained forensic experts: Necessary for analysis, but uninterrupted chain of custody takes precedence for legal evidence.
- * D. Expert forensic witness: Important for interpreting evidence but secondary to evidence admissibility.

EC-Council CISO Reference:

Emphasizes the importance of maintaining the integrity and admissibility of digital evidence through proper chain of custody protocols.

NEW QUESTION: 243

Which of the following most commonly falls within the scope of an information security governance steering committee?

- A. Approving access to critical financial systems
- B. Developing content for security awareness programs
- C. Interviewing candidates for information security specialist positions
- D. Vetting information security policies

Answer: D (LEAVE A REPLY)

Role of Governance Steering Committees:

Information security governance steering committees oversee the creation, approval, and maintenance of security policies. They ensure that policies align with organizational objectives and regulatory requirements.

Policy Vetting as a Core Function:

- * Ensures policies are comprehensive, relevant, and enforceable.
- * Addresses the balance between security and operational efficiency.

Why Other Options Are Incorrect:

- * A. Approving Access: This is typically handled by access control processes or data owners.
- * B. Security Awareness Programs: Content development is operational, not governance.
- * C. Interviewing Candidates: Staffing decisions are usually outside the committee's scope.

References:

EC-Council underscores policy governance as a fundamental responsibility of information security steering committees

NEW QUESTION: 244

Which publication serves as a resource of enterprise security-based standards and BEST practices?

- A. ISO 27004
- B. PCI DSS
- C. NIS Standard Publication 800-53 R5
- D. HIPAA

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 245

Which of the following is the MOST effective method to measure the effectiveness of security controls in a perimeter network?

- A. Implement network intrusion prevention systems
- B. External penetration testing by an independent third party
- C. Performing a vulnerability scan of servers using current tools and processes
- D. Internally review firewall configurations

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, the most effective way to measure the real-world effectiveness of perimeter security controls is through external penetration testing conducted by an independent third party.

CCISO materials stress that leadership-level assurance requires objective validation, not internal self-assessment. Independent penetration testing simulates real attacker behavior, techniques, and attack paths, providing executive leadership with an accurate assessment of how perimeter defenses perform under adversarial conditions.

Implementing intrusion prevention systems (Option A) is a preventive control, not a measurement method.

Vulnerability scanning (Option C) identifies known weaknesses but does not test exploitability or control effectiveness. Internal firewall reviews (Option D) validate configuration compliance but fail to account for unknown attack vectors, misconfigurations, or chained exploits.

The CCISO curriculum explicitly differentiates control implementation from control validation, emphasizing that penetration testing provides the highest level of assurance because it tests people, processes, and technology together.

Therefore, Option B is the most effective measurement method.

NEW QUESTION: 246

An example of professional unethical behavior is:

- A.** Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation
- B.** Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
- C.** Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes
- D.** Storing client lists and other sensitive corporate internal documents on a removable thumb drive

Answer: ([SHOW ANSWER](#))

Why This Is Unethical:

- * Removing company documents without authorization, even if intellectual property claims are disputed, violates professional and legal standards.
- * Such actions can lead to data breaches and undermine trust.

Why Not Other Options:

- * Option A: Gaining email access as part of an official investigation with proper authorization is ethical.
- * Option B: Sharing copyrighted material within a professional organization with legitimate access is not unethical.
- * Option D: Storing sensitive documents on a removable device can pose risks but is not inherently unethical unless it violates policies or regulations.

EC-Council Alignment:

Adhering to professional ethics, as outlined in the CISO framework, ensures actions are compliant with legal and organizational standards.

NEW QUESTION: 247

An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

- A.** Procedural control
- B.** Management control
- C.** Technical control
- D.** Administrative control

Answer: ([SHOW ANSWER](#))

Background Checks as Security Controls:

* Background checks are administrative controls because they pertain to policies and procedures designed to manage personnel security.

Purpose:

* These checks aim to verify the trustworthiness of individuals accessing sensitive systems or data.

Supporting Reference:

* CCISO defines administrative controls as processes and guidelines that include personnel management and access authorization measures.

NEW QUESTION: 248

When assessing internal control objectives, what are the auditor's PRIMARY concerns?

- A. Confidence, data telemetry, cost
- B. Compliance, effectiveness, efficiency
- C. Confidentiality, accessibility, integrity
- D. Communications, reliability, cost

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 250-300 Words Explanation From Exact Extract from Chief Information Security Officer (CCISO) Documents:

According to the EC-Council CCISO Body of Knowledge, an auditor's primary concern when assessing internal control objectives is whether controls ensure compliance, operate with effectiveness, and do so with efficiency. These three principles form the foundation of internal control evaluation across governance, risk, and audit disciplines.

Compliance ensures that controls meet regulatory, legal, contractual, and policy requirements. Auditors evaluate whether controls align with applicable standards such as ISO, NIST, or regulatory mandates.

Effectiveness measures whether controls actually achieve their intended purpose-reducing risk, preventing misuse, or detecting issues. Efficiency assesses whether controls achieve results without unnecessary cost, complexity, or operational burden.

The CCISO framework emphasizes that auditors do not design controls; they evaluate whether controls are appropriately designed and functioning as intended. While confidentiality, integrity, and availability are core security objectives, they are outcomes of effective controls-not audit objectives themselves. Cost and communication are considerations but not primary internal control objectives.

Therefore, compliance, effectiveness, and efficiency represent the auditor's core evaluation criteria and are the correct answer.

NEW QUESTION: 249

What is the PRIMARY difference between encryption and tokenization?

- A. Encryption can be mathematically reversed to provide the original information
- B. Tokens contain all original information
- C. Tokenization can be mathematically reversed to provide the original information

D. Tokenization and hashing are better than encryption

Answer: A ([LEAVE A REPLY](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge clearly defines the primary difference between encryption and tokenization as the ability to mathematically reverse encryption using a cryptographic key to retrieve the original data. Encryption relies on mathematical algorithms and keys, allowing authorized users to decrypt the ciphertext back into its original plaintext form. According to CCISO documentation, encryption is a reversible process that protects data confidentiality while maintaining data usability. It is widely used to protect sensitive information such as personally identifiable information (PII), financial data, and intellectual property during storage and transmission. The security of encryption is dependent on key management, algorithm strength, and proper implementation.

In contrast, tokenization replaces sensitive data with a random, non-mathematical token that has no exploitable meaning outside of a controlled token vault. CCISO guidance emphasizes that tokenization does not use a mathematical algorithm to protect data. Instead, the original value is stored securely and mapped to a token. As a result, tokenization cannot be mathematically reversed, which makes option C incorrect.

Option B is incorrect because tokens do not contain original information; they merely reference it. Option D is incorrect because hashing and tokenization serve different purposes and are not universally "better" than encryption-CCISO stresses that security controls must be selected based on business requirements and risk context.

In summary, CCISO confirms that the primary distinguishing factor is that encryption is mathematically reversible, while tokenization is not.

NEW QUESTION: 250

Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

- A.** They are objective and can express risk / cost in real numbers
- B.** They are subjective and can be completed more quickly
- C.** They are objective and express risk / cost in approximates
- D.** They are subjective and can express risk /cost in real numbers

Answer: ([SHOW ANSWER](#)**)**

Quantitative Risk Assessment:

* This approach uses numerical data to measure and analyze risks, providing objective, precise results expressed in real numbers such as financial values.

Advantages Over Qualitative Assessments:

* Quantitative assessments allow for more accurate cost-benefit analyses, which are essential for budgeting and resource allocation.

Supporting Reference:

* CCISO emphasizes the utility of quantitative risk assessments for financial planning and communicating risk to stakeholders.

NEW QUESTION: 251

What is the MAIN responsibility of the purple security testing team?

- A. They emulate hackers to compromise systems
- B. They defend against simulated hacker attacks
- C. They oversee security testing and results
- D. They integrate the defensive findings and controls from the Blue Team with the threats and vulnerabilities found by the Red Team

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 252

In which of the following examples would an organization be more willing to accept a risk instead of mitigating it?

- A. The risk tolerance within the organization is high
- B. The organization's risk tolerance is low
- C. The organization primarily uses qualitative risk measurement
- D. The organization's risk management program is mature

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, risk acceptance is most likely when an organization has a high risk tolerance. Risk tolerance reflects how much uncertainty or potential loss leadership is willing to accept in pursuit of business objectives.

CCISO materials explain that organizations with high risk tolerance may accept risks when mitigation costs exceed potential impact or when risk aligns with strategic goals. Low risk tolerance (Option B) leads to mitigation or avoidance. Qualitative risk measurement (Option C) does not determine treatment decisions. A mature risk program (Option D) improves decision quality but does not inherently favor acceptance.

Therefore, Option A is correct.

NEW QUESTION: 253

The ability to require implementation and management of security controls within third-party provided services is a critical part of:

- A. Disaster recovery
- B. Vendor management
- C. Security Governance
- D. Compliance management

Answer: ([SHOW ANSWER](#))

* Vendor management focuses on the oversight of third-party providers. This includes ensuring they meet security standards, contractual obligations, and comply with relevant regulations. Requiring implementation and management of security controls is a key part of this process. Let's look at why the other options are less suitable:

- * Disaster recovery is about restoring services after an outage. While security is important in disaster recovery, it's not the primary focus of requiring security controls in third-party services.
- * Security governance is a broader framework of policies and processes for managing organizational security. While vendor management falls under it, it's not the specific aspect highlighted in the question.
- * Compliance management ensures adherence to laws and regulations. It's related to vendor management, but the question focuses specifically on the ability to require security controls, which is a vendor management function.

NEW QUESTION: 254

Which of the following is the MOST effective technology to counter phishing attacks?

- A. Vulnerability scanning software
- B. Additional monitoring of low-risk individuals
- C. Email anti-spam solutions
- D. Email antivirus solutions

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation:

CCISO materials identify email anti-spam solutions as the most effective technical control against phishing.

Anti-spam solutions use reputation analysis, content inspection, and behavioral analysis to block phishing before delivery.

Antivirus solutions typically detect malware payloads, not social engineering attacks. Therefore, email anti-spam solutions are the best answer.

NEW QUESTION: 255

What is the MOST critical output of the incident response process?

- A. A complete document of all involved team members and the support they provided
- B. Recovery of all data from affected systems
- C. Lessons learned from the incident, so they can be incorporated into the incident response processes
- D. Clearly defined documents detailing standard evidence collection and preservation processes

Answer: ([SHOW ANSWER](#))

The most critical output of the incident response process is the lessons learned. These lessons help refine incident response plans, prevent recurrence, and improve organizational resilience. While documenting team activities, recovering data, and detailing evidence processes (A, B, D) are important, they do not provide the proactive improvement that lessons learned offer for future incident handling.

Reference: <https://www.eccouncil.org/incident-response-plan-phases/>

NEW QUESTION: 256

Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?

- A. Trusted and untrusted networks
- B. Type of authentication
- C. Storage encryption
- D. Log retention

Answer: (SHOW ANSWER)

Tuning an Intrusion Detection System (IDS) is a critical task that ensures optimal detection of malicious activities while minimizing false positives and false negatives. The most important factor during this process is distinguishing between trusted and untrusted networks because IDS relies heavily on understanding traffic sources and destinations to differentiate legitimate traffic from potential threats.

* Identification of Network Zones:

* Trusted networks usually include internal enterprise systems with known, monitored activity.

* Untrusted networks refer to external sources such as the internet or third-party services that may harbor threats.

* Baseline Definition:

* By clearly defining what constitutes normal behavior for trusted and untrusted zones, an IDS can be configured to flag anomalies effectively.

* Ruleset Customization:

* Trusted zones require minimal scrutiny for legitimate internal communications, while untrusted zones often need stricter monitoring.

* Reduction of False Positives:

* Misclassification between trusted and untrusted zones can lead to excessive alerts or overlooked threats. Proper tuning reduces these errors.

* Threat Intelligence Integration:

* Ensuring proper network classifications allows seamless integration of threat intelligence feeds, providing accurate detection in untrusted zones while maintaining efficiency in trusted zones.

* Detection and Response: EC-Council emphasizes that understanding network boundaries and applying them to security mechanisms, such as IDS, is crucial for effective threat detection.

* Network Security Architecture: In EC-Council's methodologies, classification of trusted/untrusted networks forms the foundation for creating robust security policies.

* Strategic Risk Management: Identifying zones also aids in aligning IDS tuning with broader organizational risk management strategies.

By focusing on trusted and untrusted network delineation during IDS tuning, organizations ensure that their detection systems are both effective and efficient. This process aligns with EC-Council's principles of maintaining a balance between proactive detection and operational manageability.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!

ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest**

ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (639 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 257

What is the relationship between information protection and regulatory compliance?

- A. That all information in an organization must be protected equally.
- B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
- C. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.
- D. There is no relationship between the two.

Answer: C (LEAVE A REPLY)

Dual Nature of Information Protection:

- * Regulatory requirements mandate the protection of specific data types, such as personally identifiable information (PII) or national ID numbers, to comply with laws like GDPR or CCPA.
- * Other types of sensitive data, like trade secrets, are protected based on the organization's business needs and strategic interests.

Integration with Data Classification Policies:

- * Data classification policies should identify and prioritize regulatory compliance needs alongside business priorities.

Supporting Reference:

- * EC-Council CCISO materials emphasize aligning data protection practices with both regulatory and organizational objectives.

NEW QUESTION: 258

ABC Limited has recently suffered a security breach with customers' social security number available on the dark web for sale. The CISO, during the time of the incident, has been fired, and you have been hired as the replacement. The analysis of the breach found that the absence of an insider threat program, lack of least privilege policy, and weak access control was to blame. You would like to implement key performance indicators to mitigate the risk.

Which metric would meet the requirement?

- A. Number of times third parties access critical information systems
- B. Number of systems with known vulnerabilities
- C. Number of users with elevated privileges
- D. Number of websites with weak or misconfigured certificates

Answer: (SHOW ANSWER)

- * Relevance to the Breach:
- * The analysis highlighted insider threats, lack of least privilege, and weak access controls as root causes.

* Monitoring and minimizing the number of users with elevated privileges directly addresses these vulnerabilities.

* Why Not Other Options:

* A: Monitoring third-party access is important but not directly tied to insider threats.

* B: Vulnerability management is relevant but unrelated to least privilege or access control.

* D: Certificate issues pertain to encryption, not insider threats or access controls.

References:

EC-Council CISO Handbook: Metrics for Access Control and Insider Threat Management.

NEW QUESTION: 259

Which of the following provides an independent assessment of a vendor's internal security controls and overall posture?

A. Alignment with business goals

B. ISO27000 accreditation

C. PCI attestation of compliance

D. Financial statements

Answer: B ([LEAVE A REPLY](#))

ISO27000 Accreditation

* ISO 27000 standards provide a framework for assessing and certifying an organization's information security management systems (ISMS).

* An independent body evaluates the organization's compliance with ISO standards, ensuring robust security controls.

Comparison of Options

* A. Alignment with business goals: Not specific to security controls assessment.

* C. PCI attestation of compliance: Focuses on payment card industry standards, not general vendor security posture.

* D. Financial statements: Provide financial insights but not security assessments.

EC-Council References

* Highlighted as a benchmark for third-party risk management in EC-Council CISO training.

NEW QUESTION: 260

What would be the MOST likely reason a CISO sees abnormally high volumes of security exceptions within a number of business functions?

A. Weak audit support for the security program

B. This is normal since business units resist security requirements

C. A lack of executive presence within the security program

D. Poor alignment of the security program to the organization

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words)

According to EC-Council CCISO documentation, the most common root cause of high volumes of security exceptions is poor alignment between the security program and the organization's business operations.

CCISO materials emphasize that when security controls do not align with business workflows, objectives, or risk tolerance, business units are forced to request exceptions to operate effectively. This signals a governance failure, not user resistance.

Weak audit support (Option A) affects oversight, not exception volume. Business resistance (Option B) is an oversimplification rejected by CCISO governance principles. Lack of executive presence (Option C) may exacerbate the issue, but the underlying cause remains misalignment. CCISO training stresses that effective security programs are risk-based, business-aware, and adaptable. High exception rates are a leading indicator that controls are impractical, poorly designed, or not mapped to business needs.

Therefore, Option D is the correct answer.

NEW QUESTION: 261

Which of the following is the BEST reason for CISO collaboration with legal, IT, and core business functions?

- A.** To include as many people as possible with security decisions
- B.** To make sure all regulatory requirements are distributed to all stakeholders in the business
- C.** To allow for faster acquisition of security services and products
- D.** To provide integration of the security program to the business

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge emphasizes that the primary reason a CISO collaborates with legal, IT, and core business functions is to integrate the security program into the business. CCISO guidance consistently stresses that information security must be embedded into business processes, decision-making, and strategy rather than operating as an isolated technical function.

Collaboration with legal ensures regulatory, contractual, and liability considerations are addressed.

Engagement with IT enables effective implementation of controls and operational alignment. Coordination with business units ensures security supports revenue generation, operational efficiency, and risk tolerance.

CCISO materials state that this integration enables security to act as a business enabler, not a blocker.

Other options describe secondary benefits, but none represent the core objective. Therefore, integration of the security program into the business is the best reason.

NEW QUESTION: 262

What is the estimate of all direct and indirect costs associated with an asset or acquisition over its entire life cycle?

- A. Return on Investment
- B. Total Cost of Ownership
- C. Total COST of Product
- D. Total Cost of Production

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 263

Which of the following represents the best method of ensuring business unit alignment with security program requirements?

- A. Provide clear communication of security requirements throughout the organization
- B. Demonstrate executive support with written mandates for security policy adherence
- C. Create collaborative risk management approaches within the organization
- D. Perform increased audits of security processes and procedures

Answer: ([SHOW ANSWER](#))

Collaborative Risk Management:

A collaborative approach ensures that security requirements are integrated into business operations while addressing the needs of all stakeholders.

Key Considerations:

- * Involves engaging business units to identify risks and jointly develop mitigation strategies.
- * Fosters a sense of shared responsibility for security outcomes.

Why Not Other Options:

- * Communication (A) is essential but does not ensure alignment.
- * Executive mandates (B) may create compliance but not collaboration.
- * Increased audits (D) do not foster alignment and may create friction.

EC-Council CISO Guidance:

Collaborative approaches ensure that security programs are viewed as partners in achieving organizational goals.

NEW QUESTION: 264

Who should be involved in the development of an internal campaign to address email phishing?

- A. Business unit leaders, CIO, CEO
- B. Business Unit Leaders, CISO, CIO and CEO
- C. All employees
- D. CFO, CEO, CIO

Answer: ([SHOW ANSWER](#))

- * Collaborative Development of Anti-Phishing Campaigns:
- * Business Unit Leaders: Understand operational needs and provide input on specific risks.
- * CISO: Designs the campaign and ensures alignment with security policies.
- * CIO: Ensures IT systems and training are available for campaign execution.

- * CEO: Champions the campaign, ensuring organizational buy-in.
- * Why Not Other Options:
- * A & D: CFO's role is unrelated to phishing awareness campaigns.
- * C: All employees participate but do not develop the campaign.

References:

EC-Council CISO Material: Security Awareness and Phishing Campaign Development.

NEW QUESTION: 265

A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

- A.** If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
- B.** If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
- C.** If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
- D.** If the findings do not impact regulatory compliance, review current security controls.

Answer: (SHOW ANSWER)

Regulatory Compliance Priority:

Compliance-related findings are typically high priority because they directly impact the organization's legal and operational obligations. The EC-Council CISO curriculum emphasizes that compliance issues must be addressed promptly to avoid penalties, reputational damage, and legal consequences.

Focus on High-Impact Findings:

High-impact findings often represent the most critical risks to the organization, whether due to potential financial, operational, or reputational harm. Resolving these first aligns with risk management best practices as outlined in the EC-Council CISO program.

Remediation Steps:

- * Identify which findings impact regulatory compliance.
- * Prioritize high-impact findings for immediate remediation.
- * Develop a remediation plan that aligns with regulatory and organizational risk thresholds.

EC-Council CISO Emphasis:

This approach ensures alignment with compliance and strategic risk mitigation while fostering regulatory confidence.

NEW QUESTION: 266

The total cost of security controls should:

- A.** Be equal to the value of the information resource being protected
- B.** Be greater than the value of the information resource being protected
- C.** Be less than the value of the information resource being protected
- D.** Should not matter, as long as the information resource is protected

Answer: (SHOW ANSWER)

The total cost of security controls must always be less than the value of the protected asset, ensuring cost- effectiveness in resource allocation.

* Economic Principle of Security:

* Spending more to protect an asset than its value undermines the financial justification for security.

* Cost-Benefit Consideration:

* Security investments should provide value greater than their cost by reducing potential losses and improving operational resilience.

* Relevance of Other Options:

* Equal to Value: Break-even point but not cost-efficient.

* Greater than Value: Leads to inefficiencies.

* Should Not Matter: Contradicts sound financial practices.

* Economic Feasibility of Security Measures: Discusses balancing security costs with asset value.

* Risk-Driven Decision Making: Guides the alignment of resource allocation with organizational goals and asset value.

NEW QUESTION: 267

As the CISO, you are the project sponsor for a highly visible log management project. The objective of the project is to centralize all the enterprise logs into a security information and event management (SIEM) system. You requested the results of the performance quality audits activity. The performance quality audit activity is done in what project management process group?

- A. Executing
- B. Controlling
- C. Planning
- D. Closing

Answer: B (LEAVE A REPLY)

* Performance Quality Audits in Project Management:

* Audits are conducted during the controlling process group to ensure the project is on track and quality standards are met.

* Controlling involves monitoring and measuring performance against plans and taking corrective action when necessary.

* Why Not Other Options:

* A: Executing focuses on delivering work, not performance audits.

* C: Planning involves preparing, not monitoring.

* D: Closing addresses finalizing the project, not performance checks.

Reference:

Master of Project Management Blog: Process Groups in Project Management Reference:

[https://blog.masterofproject.com/executing-process-group-project-management/#:~:](https://blog.masterofproject.com/executing-process-group-project-management/#:~:text=Executing%20Process%20Group%20Activity%20%2310,of%20the%20project%20are%20met)

[text=Executing%20Process%20Group%20Activity%20%2310,of%20the%20project%20are%20met](https://blog.masterofproject.com/executing-process-group-project-management/#:~:text=Executing%20Process%20Group%20Activity%20%2310,of%20the%20project%20are%20met)

NEW QUESTION: 268

Which of the following are the triple constraints of project management?

- A. Time, quality, and scope
- B. Cost, quality, and time
- C. Scope, time, and cost
- D. Quality, scope, and cost

Answer: (SHOW ANSWER)

The triple constraints of project management, also known as the "iron triangle," are scope, time, and cost.

These three constraints are interdependent:

- * Scope: Defines what the project will deliver.
- * Time: Represents the project schedule and deadlines.
- * Cost: Encompasses the budget and financial resources required.

Balancing these constraints is critical for project success.

Reference: [https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%](https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%20of,scope%2C%20time%2C%20and%20cost)

[20or%20point%20of,scope%2C%20time%2C%20and%20cost](https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%20of,scope%2C%20time%2C%20and%20cost)

NEW QUESTION: 269

Which of the following statements about Encapsulating Security Payload (ESP) is true?

- A. It is an IPSec protocol.
- B. It is a text-based communication protocol.
- C. It uses TCP port 22 as the default port and operates at the application layer.
- D. It uses UDP port 22

Answer: (SHOW ANSWER)

Encapsulating Security Payload (ESP):

ESP is a protocol within the IPSec suite that provides confidentiality, integrity, and authentication for network traffic by encrypting packet payloads.

Key Features of ESP:

- * Operates at the network layer.
- * Ensures data confidentiality and protects against tampering.

Why Not Other Options:

- * B. Text-based communication protocol: ESP is not text-based; it deals with encrypted data.
- * C. Uses TCP port 22: ESP does not operate at the application layer.
- * D. Uses UDP port 22: Incorrect; ESP typically uses protocol number 50.

EC-Council Emphasis:

ESP's role in securing IP communications highlights its importance in modern security architectures.

NEW QUESTION: 270

Which risk analysis method is the MOST effective for determining the exact financial impact of risks in an organization?

- A. Vulnerability scanning
- B. Quantitative risk analysis
- C. Qualitative risk analysis
- D. Penetration testing

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (250-350 words) From Exact Extract from Chief Information Security Officer (CCISO) Documents:

The EC-Council CCISO Body of Knowledge identifies quantitative risk analysis as the most effective method for determining the exact financial impact of risks. CCISO materials state that quantitative analysis assigns monetary values to asset loss, likelihood, and exposure, enabling precise cost-benefit decisions.

Qualitative methods use descriptive scales and cannot calculate exact financial impact.

Vulnerability scanning and penetration testing identify weaknesses but do not quantify business loss. Therefore, quantitative risk analysis is correct.

NEW QUESTION: 271

Annual Loss Expectancy is derived from the function of which two factors?

- A. Annual Rate of Occurrence and Asset Value
- B. Single Loss Expectancy and Exposure Factor
- C. Safeguard Value and Annual Rate of Occurrence
- D. Annual Rate of Occurrence and Single Loss Expectancy

Answer: (SHOW ANSWER)

Definition of Annual Loss Expectancy (ALE)

* ALE is a quantitative risk analysis metric used to estimate the annual financial impact of a risk.

* Formula: $ALE = \text{Annual Rate of Occurrence (ARO)} \times \text{Single Loss Expectancy (SLE)}$ Key

Components

* Annual Rate of Occurrence (ARO): The estimated frequency of a specific risk occurring in a year.

* Single Loss Expectancy (SLE): The financial impact of a single occurrence of the risk, calculated as $\text{Asset Value} \times \text{Exposure Factor}$.

Comparison of Options

* A. Annual Rate of Occurrence and Asset Value: Asset Value is used indirectly in SLE but not directly with ARO.

* B. Single Loss Expectancy and Exposure Factor: These factors combine to calculate SLE, not ALE.

* C. Safeguard Value and Annual Rate of Occurrence: Safeguard Value is unrelated to ALE calculation.

EC-Council References

* EC-Council frameworks and CISO resources consistently highlight ALE as a critical tool for financial risk assessment.

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!
ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (**639** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 272

Effective information security management programs require the active involvement of _____

- A. CIOS
- B. Security Managers
- C. All employees
- D. Executives

Answer: ([SHOW ANSWER](#))

Valid 712-50 Dumps shared by ExamDiscuss.com for Helping Passing 712-50 Exam!
ExamDiscuss.com now offer the **newest 712-50 exam dumps**, the ExamDiscuss.com 712-50 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 712-50 dumps with Test Engine here: <https://www.examdiscuss.com/EC-COUNCIL/exam/712-50/premium/> (**639** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)