ISACA.CISM.v2024-04-30.q329

Exam Code:	CISM
Exam Name:	Certified Information Security Manager
Certification Provider:	ISACA
Free Question Number:	329
Version:	v2024-04-30
# of views:	1505
# of Questions views:	72865
https://www.freecram.net/torrent/ISACA.CISM.v2024-04-30.q329.html	

NEW QUESTION: 1
Which of the following eradication methods is MOST appropriate when responding to an incident resulting in malware on an application server?
A. Disconnect the system from the network.
B. Change passwords on the compromised system.
C. Restore the system from a known good backup.
D. Perform operation system hardening.
Answer: (SHOW ANSWER)
Explanation
Restoring the system from a known good backup is the most appropriate eradication method when responding to an incident resulting in malware on an application server, as it ensures that the system is free of any malicious code and that the data and applications are consistent with the expected state. Disconnecting the system from the network may prevent further spread of the malware, but it does not eradicate it from the system. Changing passwords on the compromised system may reduce the risk of unauthorized access, but it does not remove the malware from the system. Performing operation system hardening may improve the security configuration of the system, but it does not guarantee that the malware is eliminated from the system.
References = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.4

NEW QUESTION: 2
Which of the following Is MOST useful to an information security manager when conducting a post-incident review of an attack?
A. Cost of the attack to the organization
B. Location of the attacker
C. Method of operation used by the attacker
D. Details from intrusion detection system (IDS) logs
Answer: (SHOW ANSWER)
Explanation

= The method of operation used by the attacker is the most useful information for an information security manager when conducting a post-incident review of an attack. This information can help identify the root cause of the incident, the vulnerabilities exploited, the impact and severity of the attack, and the effectiveness of the existing security controls. The method of operation can also provide insights into the attacker's motives, skills, and resources, which can help improve the organization's threat intelligence and risk assessment. The cost of the attack to the organization, the location of the attacker, and the details from IDS logs are all relevant information for a post-incident review, but they are not as useful as the method of operation for improving the incident handling process and preventing future attacks. References = CISM Review Manual 2022, page 316; CISM Item Development Guide 2022, page 9; ISACA CISM: PRIMARY goal of a post-incident review should be to?

NEW QUESTION: 3
Which of the following is the BEST method to protect against emerging advanced persistent threat (APT) actors?
A. Providing ongoing training to the incident response team
B. Implementing proactive systems monitoring
C. Implementing a honeypot environment
D. Updating information security awareness materials
Answer: (SHOW ANSWER)
Explanation
= Proactive systems monitoring is the best method to protect against emerging APT actors because it can help detect and respond to anomalous or malicious activities on the network, such as unauthorized access, data exfiltration, malware infection, or command and control communication. Proactive systems monitoring can also help identify the source, scope, and impact of an APT attack, as well as provide evidence for forensic analysis and remediation. Proactive systems monitoring can include tools such as intrusion detection and prevention systems (IDPS), security information and event management (SIEM) systems, network traffic analysis, endpoint detection and response (EDR), and threat intelligence feeds.
References = CISM Review Manual 15th Edition, page 201-2021; CISM Practice Quiz, question 922

NEW QUESTION: 4
Which of the following has the GREATEST influence on the successful integration of information security within the business?
A. Organizational structure and culture
B. Risk tolerance and organizational objectives
C. The desired state of the organization
D. Information security personnel
Answer: (SHOW ANSWER)
Explanation
The factor that has the greatest influence on the successful integration of information security within the business is organizational structure and culture because they determine how information security is organized, governed, and supported within the organization, and how information security roles and responsibilities are

defined, assigned, and communicated across different levels and functions. Risk tolerance and organizational objectives are not very influential because they do not affect how information security is integrated within the business, but rather what information security aims to achieve or protect. The desired state of the organization is not very influential because it does not affect how information security is integrated within the business, but rather what the organization aspires to be or do. Information security personnel are not very influential because they do not affect how information security is integrated within the business, but rather who performs information security tasks or activities. References:
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-busin

NEW QUESTION: 5
Who is BEST suited to determine how the information in a database should be classified?
A. Database analyst
B. Database administrator (DBA)
C. Information security analyst
D. Data owner
Answer: D (LEAVE A REPLY)
Explanation
= Data owner is the best suited to determine how the information in a database should be classified, because data owner is the person who has the authority and responsibility for the data and its protection. Data owner is accountable for the business value, quality, integrity, and security of the data. Data owner also defines the data classification criteria and levels based on the data sensitivity, criticality, and regulatory requirements. Data owner assigns the data custodian and grants the data access rights to the data users. Data owner reviews and approves the data classification policies and procedures, and ensures the compliance with them.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Data Classification, page 331

NEW QUESTION: 6
An organization has multiple data repositories across different departments. The information security manager has been tasked with creating an enterprise strategy for protecting data. Which of the following information security initiatives should be the HIGHEST priority for the organization?
A. Data masking
B. Data retention strategy
C. Data encryption standards
D. Data loss prevention (DLP)
Answer: (SHOW ANSWER)
Explanation
Data encryption standards are the best information security initiative for creating an enterprise strategy for protecting data across multiple data repositories and different departments because they help to ensure the confidentiality, integrity, and availability of data in transit and at rest. Data encryption is a process of

transforming data into an unreadable format using a secret key or algorithm, so that only authorized parties can access and decrypt it. Data encryption standards are the rules or specifications that define how data encryption should be performed, such as the type, strength, and mode of encryption, the key management and distribution methods, and the compliance requirements. Data encryption standards help to protect data from unauthorized access, modification, or theft, as well as to meet the regulatory obligations for data privacy and security.
Therefore, data encryption standards are the correct answer.
References:
https://www.techtarget.com/searchdatabackup/tip/20-keys-to-a-successful-enterprise-data-protection-strate
https://cloudian.com/guides/data-protection/data-protection-strategy-10-components-of-an-effective-strate
https://www.veritas.com/information-center/enterprise-data-protection

NEW QUESTION: 7
Prior to implementing a bring your own device (BYOD) program, it is MOST important to:
A. select mobile device management (MDM) software.
B. survey employees for requested applications.
C. develop an acceptable use policy.
D. review currently utilized applications.
Answer: (SHOW ANSWER)
Explanation
Before implementing a BYOD program, it is most important to develop an acceptable use policy that defines the roles and responsibilities of the organization and the employees, the security requirements and controls for the devices, the acceptable and unacceptable behaviors and activities, and the consequences of non-compliance. This policy will help to establish a clear and consistent framework for managing the risks and benefits of BYOD.
References = CISM Review Manual, 16th Edition, page 197

NEW QUESTION: 8
What is the role of the information security manager in finalizing contract negotiations with service providers?
A. To perform a risk analysis on the outsourcing process
B. To obtain a security standard certification from the provider
C. To update security standards for the outsourced process
D. To ensure that clauses for periodic audits are included
Answer: (SHOW ANSWER)
Explanation
The role of the information security manager in finalizing contract negotiations with service providers is to ensure that the outsourcing process is aligned with the organization's information security policies, standards, and objectives. One of the key aspects of this process is to perform a risk analysis on the outsourcing process, which involves identifying, assessing, and mitigating the potential threats and vulnerabilities that may arise from outsourcing activities. A risk analysis can help the information security manager to determine the appropriate level of security controls and requirements for the outsourced process, as well as to monitor and

evaluate its performance and compliance. A risk analysis can also help to avoid or minimize legal, financial, reputational, or operational risks associated with outsourcing1. References = CISM Review Manual (Digital Version), Chapter 6: Information Security Program Management CISM Review Manual (Print Version), Chapter 6: Information Security Program Management

NEW QUESTION: 9
Which of the following should be the PRIMARY basis for an information security strategy?
A. The organization's vision and mission
B. Results of a comprehensive gap analysis
C. Information security policies
D. Audit and regulatory requirements
Answer: (SHOW ANSWER)
Explanation
The organization's vision and mission should be the PRIMARY basis for an information security strategy, as they define the purpose and direction of the organization and its information security needs. A comprehensive gap analysis is a tool to identify the current state and desired state of information security, and the actions needed to close the gap. Information security policies are the high-level statements of management's intent and expectations for information security, and are derived from the information security strategy. Audit and regulatory requirements are external factors that influence the information security strategy, but are not the primary basis for it. References = CISM Review Manual, 16th Edition, pages 17-181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 782 The primary basis for an information security strategy should be the organization's vision and mission. The organization's vision and mission should be the foundation for the security strategy, and should inform and guide the security policies, procedures, and practices that are implemented. The results of a comprehensive gap analysis, information security policies, and audit and regulatory requirements should all be taken into consideration when developing the security strategy, but should not be the primary basis.

NEW QUESTION: 10
Which of the following presents the GREATEST challenge to a security operations center's wna GY of potential security breaches?

A. IT system clocks are not synchronized with the centralized logging server.
B. Operating systems are no longer supported by the vendor.
C. The patch management system does not deploy patches in a timely manner.
D. An organization has a decentralized data center that uses cloud services.
Answer: (SHOW ANSWER)
Explanation
A security operations center (SOC) relies on the centralized logging server to collect, store, analyze and correlate security events from various sources such as firewalls, intrusion detection systems, antivirus software, etc. The centralized logging server uses the timestamps of the events to perform the analysis and correlation. If the IT system clocks are not synchronized with the centralized logging server, the SOC will face difficulties in identifying the sequence and causality of the events, which will affect its ability to detect and

respond to potential security breaches. Therefore, this presents the greatest challenge to the SOC's awareness of potential security breaches.
Operating systems that are no longer supported by the vendor may pose a security risk, but they can be mitigated by applying compensating controls such as isolation, segmentation, monitoring, etc. The patch management system that does not deploy patches in a timely manner may also increase the vulnerability exposure, but it can be remediated by prioritizing and applying the critical patches as soon as possible. An organization that has a decentralized data center that uses cloud services may face some challenges in ensuring the security and compliance of the cloud environment, but it can leverage the cloud service provider's security capabilities and tools to enhance the SOC's visibility and control. Therefore, these options are not the greatest challenges to the SOC's awareness of potential security breaches. References = CISM Certified Information Security Manager Study Guide, Chapter 8: Security Operations and Incident Management, page 2691; CISM Foundations: Module 4 Course, Part One: Security Operations and Incident Management2; RSI Security, Common Challenges of SOC Teams3; Infosec Matter, Security Operations Center: Challenges of SOC Teams4

NEW QUESTION: 11
What is the BEST way to reduce the impact of a successful ransomware attack?
A. Perform frequent backups and store them offline.
B. Purchase or renew cyber insurance policies.
C. Include provisions to pay ransoms ih the information security budget.
D. Monitor the network and provide alerts on intrusions.
Answer: (SHOW ANSWER)
Explanation
Performing frequent backups and storing them offline is the best way to reduce the impact of a successful ransomware attack, as this allows the organization to restore its data and systems without paying the ransom or losing valuable information. Purchasing or renewing cyber insurance policies may help cover some of the costs and losses associated with a ransomware attack, but it does not prevent or mitigate the attack itself. Including provisions to pay ransoms in the information security budget may encourage more attacks and does not guarantee the recovery of the data or the removal of the malware. Monitoring the network and providing alerts on intrusions may help detect and respond to a ransomware attack, but it does not reduce the impact of a successful attack that has already encrypted or exfiltrated the data. References = CISM Review Manual 2023, page 1661; CISM Review Questions, Answers & Explanations Manual 2023, page 312; CISM Exam Overview - Vinsys3

NEW QUESTION: 12
During the selection of a Software as a Service (SaaS) vendor for a business process, the vendor provides evidence of a globally accepted information security certification. Which of the following is the MOST important consideration?
A. The certification includes industry-recognized security controls.
B. The certification was issued within the last five years.
C. The certification is issued for the specific scope.

D. The certification is easily verified.

Answer: (SHOW ANSWER)

Explanation

The most important consideration when selecting a SaaS vendor for a business process is whether the vendor's information security certification is issued for the specific scope of the service that the organization needs. A certification that covers the entire vendor organization or a different service may not be relevant or sufficient for the organization's security requirements. The certification should also include industry-recognized security controls, be issued within a reasonable time frame, and be easily verified, but these are not as critical as the scope.

References = CISM Review Manual, 16th Edition, page 1841; 5 Top SaaS Security Certifications for SaaS Providers

NEW QUESTION: 13

An enterprise has decided to procure security services from a third-party vendor to support its information security program. Which of the following is MOST important to include in the vendor selection criteria?

A. Feedback from the vendor's previous clients

B. Alignment of the vendor's business objectives with enterprise security goals

C. The maturity of the vendor's internal control environment

D. Penetration testing against the vendor's network

Answer: (SHOW ANSWER)

Explanation

The most important thing to include in the vendor selection criteria when procuring security services from a third-party vendor is B. Alignment of the vendor's business objectives with enterprise security goals. This is because the vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. The vendor should also be able to demonstrate how their services add value, reduce risk, and enhance the performance and maturity of the enterprise's information security program. The alignment of the vendor's business objectives with enterprise security goals can help to ensure a successful and long-term partnership, and avoid any conflicts, gaps, or issues that may arise from misalignment or divergence.

The vendor should be able to understand and support the enterprise's security vision, mission, strategy, and policies, and provide services that are consistent and compatible with them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.2.1, page 1341; Third-Party Vendor Selection: If Done Right, It's a Win-Win2; Vendor Selection Criteria: Key Factors in Procurement Success3

NEW QUESTION: 14

When performing a business impact analysis (BIA), who should be responsible for determining the initial recovery time objective (RTO)?

A. External consultant

B. Information owners

C. Information security manager

D. Business continuity coordinator

Answer: (SHOW ANSWER)

Explanation

Information owners are responsible for determining the initial recovery time objective (RTO) for their information assets and processes, as they are the ones who understand the business requirements and impact of a disruption. An external consultant may assist in conducting the business impact analysis (BIA), but does not have the authority to decide the RTO. An information security manager may provide input on the security aspects of the RTO, but does not have the business perspective to determine the RTO. A business continuity coordinator may facilitate the BIA process and ensure the alignment of the RTO with the business continuity plan, but does not have the ownership of the information assets and processes. References = CISM Review Manual 15th Edition, page 202.

When performing a business impact analysis (BIA), it is the responsibility of the business continuity coordinator to determine the initial recovery time objective (RTO). The RTO is a critical component of the BIA and should be determined in cooperation with the information owners. The RTO should reflect the maximum tolerable period of disruption (MTPD) and should be used to guide the development of the recovery strategy.

NEW QUESTION: 15

When assigning a risk owner, the MOST important consideration is to ensure the owner has:

A. adequate knowledge of risk treatment and related control activities.

B. decision-making authority and the ability to allocate resources for risk.

C. sufficient time for monitoring and managing the risk effectively.

D. risk communication and reporting skills to enable decision-making.

Answer: (SHOW ANSWER)

Explanation

Comprehensive and Detailed Explanation = The risk owner is the person or entity with the accountability and authority to manage a risk. The risk owner should have the decision-making authority and the ability to allocate resources for risk treatment and related control activities. The risk owner should also be responsible for monitoring and reporting on the risk, but these are not the most important considerations when assigning a risk owner. The risk owner may not have adequate knowledge of risk treatment and related control activities, but can delegate or consult with experts as needed. The risk owner should also have sufficient time for managing the risk effectively, but this is not a prerequisite for assigning a risk owner.

References =

CISM Review Manual 15th Edition, page 76

CISM Practice Quiz, question 4171

NEW QUESTION: 16

Which of the following is the BEST course of action when confidential information is inadvertently disseminated outside the organization?

A. Review compliance requirements.

B. Communicate the exposure.

C. Declare an incident.

D. Change the encryption keys.
Answer: (SHOW ANSWER)
Explanation
Declaring an incident is the best course of action when confidential information is inadvertently disseminated outside the organization, as it triggers the incident response process, which aims to contain, analyze, eradicate, recover, and learn from the incident. Declaring an incident also helps to communicate the exposure to the relevant stakeholders, such as senior management, legal authorities, customers, or regulators, and to comply with the applicable laws and regulations regarding notification and disclosure. Changing the encryption keys, reviewing compliance requirements, or communicating the exposure are possible steps within the incident response process, but they are not the first course of action.
References = CISM Review Manual 2022, page 3121; CISM Exam Content Outline, Domain 4, Task 4.12; CISM 2020: Incident Management; How to Respond to a Data Breach

NEW QUESTION: 17
An information security manager has identified that privileged employee access requests to production servers are approved; but user actions are not logged. Which of the following should be the GREATEST concern with this situation?
A. Lack of availability
B. Lack of accountability
C. Improper authorization
D. Inadequate authentication
Answer: (SHOW ANSWER)
Explanation
The greatest concern with the situation of privileged employee access requests to production servers being approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. References:
* https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged-access-management-p
* https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices
* https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

NEW QUESTION: 18
The PRIMARY goal of the eradication phase in an incident response process is to:
A. maintain a strict chain of custody.
B. provide effective triage and containment of the incident.
C. remove the threat and restore affected systems
D. obtain forensic evidence from the affected system.
Answer: C (LEAVE A REPLY)
Explanation
The primary goal of the eradication phase in an incident response process is to remove the threat and restore affected systems because it eliminates any traces or remnants of malicious activity or compromise from the systems or network, and returns them to their normal or secure state. Maintaining a strict chain of custody is not a goal of the eradication phase, but rather a requirement for preserving and documenting digital evidence throughout the incident response process. Providing effective triage and containment of the incident is not a goal of the eradication phase, but rather a goal of the containment phase, which isolates and stops the spread of malicious activity or compromise. Obtaining forensic evidence from the affected system is not a goal of the eradication phase, but rather a goal of the identification phase, which collects and analyzes data or artifacts related to malicious activity or compromise. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 19
Which of the following BEST enables the assignment of risk and control ownership?
A. Aligning to an industry-recognized control framework
B. Adopting a risk management framework
C. Obtaining senior management buy-in
D. Developing an information security strategy
Answer: (SHOW ANSWER)
Explanation
Obtaining senior management buy-in is the best way to enable the assignment of risk and control ownership because it helps to establish the authority and accountability of the risk and control owners, as well as to provide them with the necessary resources and support to perform their roles. Risk and control ownership refers to the assignment of specific responsibilities and accountabilities for managing risks and controls to individuals or groups within the organization. Obtaining senior management buy-in helps to ensure that risk and control ownership is aligned with the organizational objectives, structure, and culture, as well as to communicate the expectations and benefits of risk and control ownership to all stakeholders. Therefore, obtaining senior management buy-in is the correct answer.
References:
https://www.protechtgroup.com/en-au/blog/risk-control-management
https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/23_getting_
https://www.linkedin.com/pulse/risk-controls-who-owns-them-david-tattam

NEW QUESTION: 20

When designing a disaster recovery plan (DRP), which of the following MUST be available in order to prioritize system restoration?

A. Business impact analysis (BIA) results

B. Key performance indicators (KPIs)

C. Recovery procedures

D. Systems inventory

Answer: (SHOW ANSWER)

Explanation

A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident, emergency, or threat. A BIA helps to determine the business continuity requirements and priorities for recovery of business functions and processes, including their dependencies on IT systems, applications, and data. A BIA also provides information on the financial and operational impacts of a disruption, the recovery time objectives (RTOs), the recovery point objectives (RPOs), and the minimum service levels for each business function and process. A BIA is an essential input for designing a disaster recovery plan (DRP), which is a documented and approved set of procedures and arrangements to enable an organization to respond to a disaster and resume its critical functions within a predetermined timeframe. A DRP must be based on the BIA results to ensure that the system restoration is prioritized according to the business needs and expectations. A DRP must also consider the availability and suitability of the recovery resources, such as backup systems, alternate sites, and personnel. A DRP should be tested and updated regularly to ensure its effectiveness and alignment with the changing business environment and requirements. References = CISM Review Manual, 15th Edition, pages 175-1761; CISM Review Questions, Answers & Explanations Database, question ID 2182; Working Toward a Managed, Mature Business Continuity Plan - ISACA3; Part Two: Business Continuity and Disaster Recovery Plans - CISM Foundations: Module 4 Course4.

A BIA is an important part of Disaster Recovery Planning (DRP). It helps identify the impact of a disruption on the organization, including the critical systems and processes that must be recovered in order to minimize that impact. The BIA results are used to prioritize system restoration and determine the resources needed to get the organization back into operation as quickly as possible.

NEW QUESTION: 21

Which of the following should be the PRIMARY focus of a status report on the information security program to senior management?

A. Providing evidence that resources are performing as expected

B. Verifying security costs do not exceed the budget

C. Demonstrating risk is managed at the desired level

D. Confirming the organization complies with security policies

Answer: (SHOW ANSWER)

Explanation

The primary focus of a status report on the information security program to senior management is to demonstrate that the risk to the organization's information assets is managed at the desired level, in alignment with the business objectives and risk appetite. This can be achieved by providing relevant and meaningful metrics, indicators, and trends that show the performance, effectiveness, and value of the information security program, as well as the current and emerging risks and the corresponding mitigation strategies. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 22
The MOST appropriate time to conduct a disaster recovery test would be after:
A. major business processes have been redesigned.
B. the business continuity plan (BCP) has been updated.
C. the security risk profile has been reviewed
D. noncompliance incidents have been filed.
Answer: B (LEAVE A REPLY)
Explanation
The most appropriate time to conduct a disaster recovery test would be after the business continuity plan (BCP) has been updated, as it ensures that the disaster recovery plan (DRP) is aligned with the current business requirements, objectives, and priorities. The BCP should be updated regularly to reflect any changes in the business environment, such as new threats, risks, processes, technologies, or regulations. The disaster recovery test should validate the effectiveness and efficiency of the DRP, as well as identify any gaps, issues, or improvement opportunities123. References =
1: CISM Review Manual 15th Edition, page 2114
2: CISM Practice Quiz, question 1042
3: Business Continuity Planning and Disaster Recovery Testing, section "Testing the Plan"

NEW QUESTION: 23
Which of the following is the MOST effective way to help staff members understand their responsibilities for information security?
A. Communicate disciplinary processes for policy violations.
B. Require staff to participate in information security awareness training.
C. Require staff to sign confidentiality agreements.
D. Include information security responsibilities in job descriptions.
Answer: (SHOW ANSWER)
Explanation
The most effective way to help staff members understand their responsibilities for information security is to require them to participate in information security awareness training. Information security awareness training is a program that educates and motivates the staff members about the importance, benefits, and principles of information security, and the roles and responsibilities that they have in protecting the information assets and resources of the organization. Information security awareness training also provides the staff members with the necessary knowledge, skills, and tools to comply with the information security policies, procedures, and standards of the organization, and to prevent, detect, and report any information security incidents or issues.

Information security awareness training also helps to create and maintain a positive and proactive information security culture among the staff members, and to increase their confidence and competence in performing their information security duties.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281; CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Awareness, Training and Education, pages 197-1982.

NEW QUESTION: 24
An organization is close to going live with the implementation of a cloud-based application. Independent penetration test results have been received that show a high-rated vulnerability. Which of the following would be the BEST way to proceed?
A. Implement the application and request the cloud service provider to fix the vulnerability.
B. Assess whether the vulnerability is within the organization's risk tolerance levels.
C. Commission further penetration tests to validate initial test results,
D. Postpone the implementation until the vulnerability has been fixed.
Answer: B (LEAVE A REPLY)
Explanation
The best way to proceed when an independent penetration test results show a high-rated vulnerability in a cloud-based application that is close to going live is to assess whether the vulnerability is within the organization's risk tolerance levels. This is because the organization should not implement the application without understanding the potential impact and likelihood of the vulnerability being exploited, and the cost and benefit of fixing or mitigating the vulnerability. The organization should also consider the contractual and legal obligations, service level agreements, and performance expectations of the cloud service provider and the application users. By assessing the risk tolerance levels, the organization can make an informed and rational decision on whether to accept, transfer, avoid, or reduce the risk, and how to allocate the resources and responsibilities for managing the risk.
Implementing the application and requesting the cloud service provider to fix the vulnerability is not the best way to proceed, because it exposes the organization to unnecessary and unacceptable risk, and it may violate the terms and conditions of the cloud service contract. The organization should not rely on the cloud service provider to fix the vulnerability, as the provider may not have the same level of urgency, accountability, or capability as the organization. The organization should also not assume that the vulnerability will not be exploited, as cyberattackers may target the cloud-based application due to its high visibility, accessibility, and value.
Commissioning further penetration tests to validate initial test results is not the best way to proceed, because it may delay the implementation of the application, and it may not provide any additional or useful information. The organization should trust the results of the independent penetration test, as it is conducted by a qualified and objective third party. The organization should also not waste time and resources on conducting redundant or unnecessary tests, as it may affect the budget, schedule, and quality of the project.
Postponing the implementation until the vulnerability has been fixed is not the best way to proceed, because it may not be feasible or desirable for the organization. The organization should consider the business impact

and opportunity cost of postponing the implementation, as it may affect the organization's reputation, revenue, and customer satisfaction. The organization should also consider the technical feasibility and complexity of fixing the vulnerability, as it may require significant changes or modifications to the application or the cloud environment. The organization should not adopt a zero-risk or risk-averse approach, as it may hinder the organization's innovation and competitiveness. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 97-98, 101-102, 105-106, 109-110.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1025.

NEW QUESTION: 25
Management decisions concerning information security investments will be MOST effective when they are based on:
A. a process for identifying and analyzing threats and vulnerabilities.
B. an annual loss expectancy (ALE) determined from the history of security events,
C. the reporting of consistent and periodic assessments of risks.
D. the formalized acceptance of risk analysis by management,
Answer: (SHOW ANSWER)
Explanation
Management decisions concerning information security investments will be most effective when they are based on the reporting of consistent and periodic assessments of risks. This will help management to understand the current and emerging threats, vulnerabilities, and impacts that affect the organization's information assets and business processes. It will also help management to prioritize the allocation of resources and funding for the most critical and cost-effective security controls and solutions. The reporting of consistent and periodic assessments of risks will also enable management to monitor the performance and effectiveness of the information security program, and to adjust the security strategy and objectives as needed. References = CISM Review Manual 15th Edition, page 28.

NEW QUESTION: 26
An organization wants to integrate information security into its HR management processes. Which of the following should be the FIRST step?
A. Benchmark the processes with best practice to identify gaps.
B. Calculate the return on investment (ROI).
C. Provide security awareness training to HR.
D. Assess the business objectives of the processes.
Answer: (SHOW ANSWER)
Explanation
The first step when integrating information security into HR management processes is to assess the business objectives of the processes, which means understanding the purpose, scope, and expected outcomes of the HR functions and activities, and how they relate to the organization's strategy and goals. The assessment will help to identify the information security requirements, risks, and controls that are relevant and applicable to the HR processes, and to align the information security objectives with the business objectives.

References = CISM Review Manual 15th Edition, CISM: Overview of domains [updated 2022]

NEW QUESTION: 27
Which of the following is the BEST method to ensure compliance with password standards?
A. Implementing password-synchronization software
B. Using password-cracking software
C. Automated enforcement of password syntax rules
D. A user-awareness program
Answer: (SHOW ANSWER)
Explanation
Automated enforcement of password syntax rules is the best method to ensure compliance with password standards. Password syntax rules define the minimum and maximum length, character types, and construction of passwords. By enforcing these rules automatically, the system can prevent users from creating or using weak or insecure passwords that do not meet the standards. According to NIST, password syntax rules should allow at least 8 characters and up to 64 characters, accept all printable ASCII characters and Unicode characters, and encourage the use of long passphrases1. The other options are not methods to ensure compliance with password standards, but rather methods to verify or improve password security.
Implementing password-synchronization software can help users manage multiple passwords across different systems, but it does not ensure that the passwords comply with the standards2. Using password-cracking software can help test the strength of passwords and identify weak or compromised ones, but it does not ensure that users follow the standards3. A user-awareness program can help educate users about the importance of password security and the best practices for creating and using passwords, but it does not ensure that users comply with the standards. References: 1: NIST Password Guidelines and Best Practices for 2020 - Auth0 2:
Password synchronization - Wikipedia 3:

NEW QUESTION: 28
Which of the following is the GREATEST challenge with assessing emerging risk in an organization?
A. Lack of a risk framework
B. Ineffective security controls
C. Presence of known vulnerabilities
D. Incomplete identification of threats
Answer: (SHOW ANSWER)
Explanation
The greatest challenge with assessing emerging risk in an organization is the incomplete identification of threats, as emerging risks are often new, unknown, or unfamiliar, and may not be fully understood or assessed.
Incomplete identification of threats can lead to gaps in risk analysis and management, and expose the organization to unexpected or unprepared scenarios. The other options, such as lack of a risk framework, ineffective security controls, or presence of known vulnerabilities, are not specific to emerging risks, and may apply to any type of risk assessment. References:

https://committee.iso.org/sites/tc262/home/projects/ongoing/iso-31022-guidelines-for-impl-2.html
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-6/emerging-risk-analys
https://projectriskcoach.com/emerging-risks/

NEW QUESTION: 29
During which phase of an incident response plan is the root cause determined?
A. Recovery
B. Lessons learned
C. Containment
D. Eradication
Answer: (SHOW ANSWER)
Explanation
The eradication phase of an incident response plan is where the root cause of the incident is determined and eliminated. This phase involves identifying and removing all traces of the malicious activity from the affected systems and restoring them to a secure state.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION: 30
Which of the following should be done FIRST when implementing a security program?
A. Perform a risk analysis
B. Implement data encryption.
C. Create an information asset inventory.
D. Determine the value of information assets.
Answer: (SHOW ANSWER)
Explanation
Performing a risk analysis is the first step when implementing a security program because it helps to identify and prioritize the potential threats and vulnerabilities that may affect the organization's assets, processes, or objectives, and determine their impact and likelihood. Implementing data encryption is not the first step, but rather a possible subsequent step that involves applying a specific security control or technique to protect data from unauthorized access or modification. Creating an information asset inventory is not the first step, but rather a possible subsequent step that involves identifying and classifying the organization's assets based on their value and sensitivity. Determining the value of information assets is not the first step, but rather a possible subsequent step that involves estimating and quantifying the worth of information assets to the organization.
References:
https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-securit
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-i

NEW QUESTION: 31

When an organization experiences a disruptive event, the business continuity plan (BCP) should be triggered PRIMARILY based on:

A. expected duration of outage.

B. management direction.

C. type of security incident.

D. the root cause of the event.

Answer: (SHOW ANSWER)

Explanation

The expected duration of outage is the primary factor that should trigger the BCP because it indicates how long the organization can tolerate the disruption of its critical business processes and functions before it causes unacceptable consequences. The expected duration of outage is determined by the recovery time objectives (RTOs) that are defined for each critical business process and function based on the business impact analysis (BIA). The BCP should be triggered when the expected duration of outage exceeds or is likely to exceed the RTOs.

References: The CISM Review Manual 2023 defines RTO as "the maximum acceptable time that a service can be unavailable or disrupted before it causes unacceptable consequences" and states that "the RTO is determined based on the impact of service interruption on the enterprise's business processes, reputation, customers, and stakeholders" (p. 189). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Expected duration of outage is the correct answer because it is the primary factor that should trigger the BCP, as it reflects the maximum time that the organization can afford to lose its critical business processes and functions without causing unacceptable consequences" (p. 96). Additionally, the article Invoking your business continuity plan: five triggers, six decision points from the ITWeb website states that "the expected duration of outage is the most important consideration when deciding to invoke the BCP, as it indicates how long the organization can sustain the disruption before it impacts its business objectives, operations, reputation, and legal obligations" (p. 2)

NEW QUESTION: 32

Which of the following metrics BEST demonstrates the effectiveness of an organization's security awareness program?

A. Percentage of employee computers and devices infected with malware

B. Number of phishing emails viewed by end users

C. Percentage of employees who regularly attend security training

D. Number of security incidents reported to the help desk

Answer: (SHOW ANSWER)

NEW QUESTION: 33
After the occurrence of a major information security incident, which of the following will BEST help an information security manager determine corrective actions?
A. Calculating cost of the incident
B. Conducting a postmortem assessment
C. Performing an impact analysis
D. Preserving the evidence
Answer: (SHOW ANSWER)
Explanation
The best way to determine corrective actions after a major information security incident is to conduct a postmortem assessment, which is a systematic and structured review of the incident, its causes, its impacts, and its lessons learned. A postmortem assessment can help to identify the root causes of the incident, the strengths and weaknesses of the incident response process, the gaps and deficiencies in the security controls, and the opportunities for improvement and remediation. A postmortem assessment can also help to document the recommendations and action plans for preventing or minimizing the recurrence of similar incidents in the future.
References = CISM Review Manual, 16th Edition eBook1, Chapter 4: Information Security Incident Management, Section: Incident Response, Subsection: Postincident Activities, Page 211.

NEW QUESTION: 34
Which of the following should be the MOST important consideration when establishing information security policies for an organization?
A. Job descriptions include requirements to read security policies.
B. The policies are updated annually.
C. Senior management supports the policies.
D. The policies are aligned to industry best practices.
Answer: (SHOW ANSWER)
Explanation
The most important consideration when establishing information security policies for an organization is to ensure that senior management supports the policies. Senior management support is essential for the successful implementation and enforcement of information security policies, as it demonstrates the commitment and accountability of the organization's leadership to information security. Senior management support also helps to allocate adequate resources, establish clear roles and responsibilities, and promote a security-aware culture within the organization. Without senior management support, information security policies may not be aligned with the organization's goals and objectives, may not be communicated and disseminated effectively, and may not be followed or enforced consistently.
Job descriptions that include requirements to read security policies are a way of ensuring that employees are aware of their security obligations, but they are not the most important consideration when establishing

information security policies. The policies should be relevant and applicable to the employees' roles and functions, and should be reinforced by regular training and awareness programs.
The policies should be updated periodically to reflect the changes in the organization's environment, risks, and requirements, but updating them annually may not be sufficient or necessary. The frequency of updating the policies should depend on the nature and impact of the changes, and should be determined by a defined policy review process.
The policies should be aligned with industry best practices, standards, and frameworks, but this is not the most important consideration when establishing information security policies. The policies should also be customized and tailored to the organization's specific context, needs, and expectations, and should be consistent with the organization's vision, mission, and values. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 37-38.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1009.

NEW QUESTION: 35
A balanced scorecard MOST effectively enables information security:
A. risk management
B. project management
C. governance
D. performance
Answer: (SHOW ANSWER)
Explanation
A balanced scorecard enables information security governance by providing a framework for aligning security objectives with business goals and measuring performance against them. The other choices are not directly related to governance but may be supported by it.
A balanced scorecard is a strategic management tool that describes the cause-and-effect linkages between four high-level perspectives of strategy and execution: financial, customer, internal process, and learning and growth2. It helps organizations communicate and monitor their vision and strategy across different levels and functions2.

NEW QUESTION: 36
Which of the following roles is PRIMARILY responsible for developing an information classification framework based on business needs?
A. Information security manager
B. Information security steering committee
C. Information owner
D. Senior management
Answer: (SHOW ANSWER)
Explanation
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.1, Information owners are responsible for developing an information classification framework based on business needs1. They are also

responsible for defining and maintaining the classification scheme, policies, and procedures for their information assets1.
The CISM Review Manual (Digital Version) also states that information owners should collaborate with other stakeholders, such as information security managers, information security steering committees, senior management, and legal counsel, to ensure that the classification framework is aligned with the organization's objectives and complies with applicable laws and regulations1.
The CISM Exam Content Outline also covers the topic of information classification frameworks in Domain 3 - Information Security Program Development and Management (27% exam weight)2. The subtopics include:
3.2.1 Information Classification Frameworks
3.2.2 Information Classification Policies
3.2.3 Information Classification Procedures
3.2.4 Information Classification Training
I hope this answer helps you prepare for your CISM exam. Good luck!

NEW QUESTION: 37
Which of the following is the PRIMARY objective of information asset classification?
A. Vulnerability reduction
B. Compliance management
C. Risk management
D. Threat minimization
Answer: (SHOW ANSWER)
Explanation
The primary objective of information asset classification is C. Risk management. This is because information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. Information asset classification also helps the organization to comply with the legal, regulatory, and contractual obligations regarding the information assets, and to optimize the use of resources and costs for information security.
Information asset classification is a process of assigning labels or categories to information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps the organization to identify, assess, and treat the risks associated with the information assets, and to apply the appropriate level of protection and controls to them. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 2, Section 2.2.1, page 751; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 7, page 3; Certified Information Security Manager Exam Prep Guide - Packt Subscription2

NEW QUESTION: 38
Which of the following is the MOST effective defense against malicious insiders compromising confidential information?
A. Regular audits of access controls

B. Strong background checks when hiring staff
C. Prompt termination procedures
D. Role-based access control (RBAC)
Answer: (SHOW ANSWER)
Explanation
role-based access control (RBAC) is the most effective defense against malicious insiders compromising confidential information, as it helps to limit the access of users to the information and resources that are necessary for their roles and responsibilities. RBAC also helps to enforce the principle of least privilege, which reduces the risk of unauthorized or inappropriate access, disclosure, modification, or destruction of information by insiders. RBAC also facilitates the monitoring and auditing of user activities and access rights.
References = Malicious insiders | Cyber.gov.au, Insider Threat Mitigation Guide - CISA, Malicious Insiders: Types, Indicators & Common Techniques - Ekran System

NEW QUESTION: 39
Which of the following is the BEST defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns?
A. Compartmentalization
B. Overlapping redundancy
C. Continuous monitoring
D. Multi-factor authentication
Answer: (SHOW ANSWER)
Explanation
Compartmentalization is the best defense-in-depth implementation for protecting high value assets or for handling environments that have trust concerns because it is a strategy that divides the network or system into smaller segments or compartments, each with its own security policies, controls, and access rules. Compartmentalization helps to isolate and protect the most sensitive or critical data and functions from unauthorized or malicious access, as well as to limit the damage or impact of a breach or compromise. Compartmentalization also helps to enforce the principle of least privilege, which grants users or processes only the minimum access rights they need to perform their tasks. Therefore, compartmentalization is the correct answer.
References:
https://www.csoonline.com/article/3667476/defense-in-depth-explained-layering-tools-and-processes-for-b
https://www.fortinet.com/resources/cyberglossary/defense-in-depth
https://sciencepublishinggroup.com/journal/paperinfo?journalid=542&doi=10.11648/j.ajai.20190302.11

NEW QUESTION: 40
Which of the following is MOST important when developing an information security strategy?
A. Engage stakeholders.
B. Assign data ownership.
C. Determine information types.
D. Classify information assets.

Answer: (SHOW ANSWER)

Explanation

Engaging stakeholders is the most important step when developing an information security strategy, as it ensures that the strategy is aligned with the business objectives, risks, and needs of the organization. Stakeholders include senior management, business units, IT staff, customers, regulators, and other relevant parties who have an interest or influence on the information security of the organization. By engaging stakeholders, the information security manager can gain their support, input, feedback, and buy-in for the strategy, as well as identify and prioritize the security requirements, expectations, and challenges.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 1

NEW QUESTION: 41

An organization is increasingly using Software as a Service (SaaS) to replace in-house hosting and support of IT applications. Which of the following would be the MOST effective way to help ensure procurement decisions consider information security concerns?

A. Integrate information security risk assessments into the procurement process.

B. Provide regular information security training to the procurement team.

C. Invite IT members into regular procurement team meetings to influence best practice.

D. Enforce the right to audit in procurement contracts with SaaS vendors.

Answer: A (LEAVE A REPLY)

Explanation

The best way to ensure that information security concerns are considered during the procurement of SaaS solutions is to integrate information security risk assessments into the procurement process. This will allow the organization to identify and evaluate the potential security risks and impacts of using a SaaS provider, and to select the most appropriate solution based on the risk appetite and tolerance of the organization. Information security risk assessments should be conducted at the early stages of the procurement process, before selecting a vendor or signing a contract, and should be updated periodically throughout the contract lifecycle.

Providing regular information security training to the procurement team (B) is a good practice, but it may not be sufficient to address the specific security issues and challenges of SaaS solutions. The procurement team may not have the expertise or the authority to conduct information security risk assessments or to negotiate security requirements with the vendors.

Inviting IT members into regular procurement team meetings to influence best practice is also a good practice, but it may not be effective if the IT members are not involved in the actual procurement process or decision making. The IT members may not have the opportunity or the influence to conduct information security risk assessments or to ensure that security concerns are adequately addressed in the procurement contracts.

Enforcing the right to audit in procurement contracts with SaaS vendors (D) is an important control, but it is not the most effective way to ensure that information security concerns are considered during the procurement process. The right to audit is a post-contractual measure that allows the organization to verify the security controls and compliance of the SaaS provider, but it does not prevent or mitigate the security risks that may arise from using a SaaS solution. The right to audit should be complemented by information security risk assessments and other security requirements in the procurement contracts.

References = CISM Review Manual (Digital Version), Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Procurement and Vendor Management, Page 141-1421

NEW QUESTION: 42

Which of the following should an information security manager do FIRST after identifying suspicious activity on a PC that is not in the organization's IT asset inventory?

A. Isolate the PC from the network

B. Perform a vulnerability scan

C. Determine why the PC is not included in the inventory

D. Reinforce information security training

Answer: C (LEAVE A REPLY)

Explanation

The first thing an information security manager should do after identifying suspicious activity on a PC that is not in the organization's IT asset inventory is to determine why the PC is not included in the inventory. This will help to identify the source and scope of the threat, as well as the potential impact and risk to the organization. The IT asset inventory is a list of all the hardware, software, data, and other resources that are owned, controlled, or used by an organization. It helps to establish accountability, visibility, and control over the IT assets, as well as to support security policies and procedures.

If a PC is not included in the inventory, it may indicate that it has been compromised by an unauthorized user or entity, or that it has been moved or transferred without proper authorization. It may also indicate that there are gaps or errors in the inventory management process, such as missing records, duplicate entries, outdated information, or inaccurate classification. These issues can pose significant challenges for information security management, such as:

Lack of visibility into the IT environment and assets

Difficulty in detecting and responding to incidents

Increased risk of data breaches and cyberattacks

Non-compliance with regulatory requirements and standards

Reduced trust and confidence among stakeholders

Therefore, an information security manager should take immediate steps to investigate why the PC is not included in the inventory and take appropriate actions to remediate the situation.

References = CISM Manual, Chapter 6: Incident Response Planning (IRP), Section 6.2: Inventory Management1

1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 43

When integrating security risk management into an organization it is MOST important to ensure:

A. business units approve the risk management methodology.

B. the risk treatment process is defined.

C. information security policies are documented and understood.

D. the risk management methodology follows an established framework.

Answer: D (LEAVE A REPLY)

Explanation

When integrating security risk management into an organization, it is most important to ensure that the risk management methodology follows an established framework, such as ISO 31000, NIST SP 800-30, or COBIT. This is because a framework provides a consistent and structured approach to identify, assess, treat, and monitor risks, and to align the risk management process with the organization's objectives, culture, and governance. A framework also helps to ensure compliance with relevant standards and regulations, and to facilitate communication and reporting of risks to stakeholders.

References: The CISM Review Manual 2023 states that "the risk management methodology should follow an established framework that provides a consistent and structured approach to risk management" and that "the framework should be aligned with the enterprise's objectives, culture, and governance, and should comply with applicable standards and regulations" (p. 94). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "The risk management methodology follows an established framework is the correct answer because it is the most important factor to ensure the successful integration of security risk management into an organization, as it provides a common language and process for managing risks across the organization" (p. 29). Additionally, the article Integrating Risk Management into Business Processes from the ISACA Journal 2018 states that "a risk management framework provides a systematic and comprehensive approach to risk management that covers the entire risk management cycle, from risk identification to risk monitoring and reporting" and that "a risk management framework should be aligned with the organization's strategy, culture, and governance, and should follow recognized standards and best practices, such as ISO 31000, NIST SP 800-30, or COBIT" (p. 1)

NEW QUESTION: 44

An information security manager learns that business unit leaders are encouraging increased use of social media platforms to reach customers. Which of the following should be done FIRST to help mitigate the risk of confidential information being disclosed by employees on social media?

A. Establish an organization-wide social media policy.

B. Develop sanctions for misuse of social media sites.

C. Monitor social media sites visited by employees.

D. Restrict social media access on corporate devices.

Answer: (SHOW ANSWER)

Explanation

An organization-wide social media policy is a document that defines the rules and guidelines for using social media platforms within the organization. It covers topics such as who can use social media, what they can post, how they should protect confidential information, and what are the consequences for violating the policy. An organization-wide social media policy helps to mitigate the risk of confidential information being disclosed by employees on social media by providing a clear and consistent framework for managing social media activities12.

References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271

NEW QUESTION: 45
What type of control is being implemented when a security information and event management (SIEM) system is installed?
A. Preventive
B. Deterrent
C. Detective
D. Corrective
Answer: (SHOW ANSWER)
Explanation
A security information and event management (SIEM) system is a type of detective control because it monitors and analyzes the security events or logs from different sources or systems, and detects any anomalies or incidents that may indicate a security breach or compromise. A preventive control is a type of control that prevents or blocks any unauthorized or malicious activity or access from occurring. A deterrent control is a type of control that discourages or warns any potential attackers or intruders from attempting any unauthorized or malicious activity or access. A corrective control is a type of control that restores or repairs any damage or disruption caused by an unauthorized or malicious activity or access. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration-testing
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 46
In order to gain organization-wide support for an information security program, which of the following is MOST important to consider?
A. Maturity of the security policy
B. Clarity of security roles and responsibilities
C. Corporate culture
D. Corporate risk framework
Answer: C (LEAVE A REPLY)
Explanation
Corporate culture is the most important factor to consider when trying to gain organization-wide support for an information security program because it reflects the values, beliefs, and behaviors of the organization and its members. Corporate culture influences how the organization perceives, prioritizes, and responds to information security risks and issues, and how it adopts and implements information security policies and practices. By understanding and aligning with the corporate culture, the information security manager can communicate the benefits and value of the information security program, and foster a positive and collaborative security culture across the organization.
References: The CISM Review Manual 2023 states that "corporate culture is the set of shared values, beliefs, and behaviors that characterize the organization and its members" and that "corporate culture affects how the organization views and manages information security risks and issues, and how it supports and implements information security policies and practices" (p. 81). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Corporate culture is the correct answer

because it is the most important factor to consider when trying to gain organization-wide support for an information security program, as it reflects the values, beliefs, and behaviors of the organization and its members, and influences how they perceive, prioritize, and respond to information security risks and issues, and how they adopt and implement information security policies and practices" (p. 23). Additionally, the article Building a Culture of Security from the ISACA Journal 2019 states that "corporate culture is the key factor that determines the success or failure of an information security program" and that "corporate culture can be either an enabler or a barrier for information security, depending on how well it aligns with the information security objectives, values, and practices of the organization" (p. 1)

NEW QUESTION: 47
A newly appointed information security manager has been asked to update all security-related policies and procedures that have been static for five years or more. What should be done NEXT?
A. Gain an understanding of the current business direction.
B. Update in accordance with the best business practices.
C. Inventory and review current security policies.
D. Perform a risk assessment of the current IT environment.
Answer: (SHOW ANSWER)

NEW QUESTION: 48
Which of the following is ESSENTIAL to ensuring effective incident response?
A. Business continuity plan (BCP)
B. Cost-benefit analysis
C. Classification scheme
D. Senior management support
Answer: (SHOW ANSWER)
Explanation
Senior management support is essential to ensuring effective incident response because it provides the necessary authority, resources, and guidance for the information security team to perform their roles and responsibilities. Senior management support also helps to establish the goals, scope, policies, and procedures for the incident response plan (IRP), as well as to ensure its alignment with the business objectives and strategy. Senior management support also fosters a culture of security awareness, accountability, and collaboration among all stakeholders involved in the incident response process.

The other options are not essential to ensuring effective incident response, although they may be helpful or beneficial. A business continuity plan (BCP) is a document that outlines the actions and arrangements to ensure the continuity of critical business functions in the event of a disruption or disaster. A cost-benefit analysis is a method of comparing the costs and benefits of different alternatives or solutions to a problem. A classification scheme is a system of categorizing information assets based on their sensitivity, value, and criticality.
References = CISM Manual1, Chapter 6: Incident Response Planning (IRP), Section 6.1: Incident Response Plan2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 4

NEW QUESTION: 49
Which of the following is MOST important to have in place as a basis for developing an effective information security program that supports the organization's business goals?
A. Metrics to drive the information security program
B. Information security policies
C. A defined security organizational structure
D. An information security strategy
Answer: (SHOW ANSWER)
Explanation
An information security strategy is the most important element to have in place as a basis for developing an effective information security program that supports the organization's business goals. An information security strategy is a high-level plan that defines the vision, mission, objectives, scope, and principles of information security for the organization1. It also aligns the information security program with the organization's strategy, culture, risk appetite, and governance framework2. An information security strategy provides the direction, guidance, and justification for the information security program, and ensures that the program is consistent, coherent, and comprehensive3. An information security strategy also helps to prioritize the information security initiatives, allocate the resources, and measure the performance and value of the information security program4.
The other options are not as important as an information security strategy, because they are either derived from or dependent on the strategy. Metrics are used to drive the information security program, but they need to be based on the strategy and aligned with the goals and objectives of the program. Information security policies are the rules and standards that implement the information security strategy and define the expected behavior and responsibilities of the stakeholders. A defined security organizational structure is the way the information security roles and functions are organized and coordinated within the organization, and it should reflect the strategy and the governance model. References = 1: CISM Review Manual 15th Edition, Chapter 1, Section
1.1 2: CISM Review Manual 15th Edition, Chapter 1, Section 1.2 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 4: CISM Review Manual 15th Edition, Chapter 1, Section 1.4 : CISM Review Manual 15th Edition, Chapter 1, Section 1.5 : CISM Review Manual 15th Edition, Chapter 1, Section 1.6 : CISM Review Manual 15th Edition, Chapter 1, Section 1.7

NEW QUESTION: 50

An organization has remediated a security flaw in a system. Which of the following should be done NEXT?

A. Assess the residual risk.

B. Share lessons learned with the organization.

C. Update the system's documentation.

D. Allocate budget for penetration testing.

Answer: (SHOW ANSWER)

Explanation

Residual risk is the risk that remains after applying controls to mitigate the original risk. It is important to assess the residual risk after remediation to ensure that it is within the acceptable level and tolerance of the organization. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

NEW QUESTION: 51

Which of the following is the MOST effective way to detect security incidents?

A. Analyze recent security risk assessments.

B. Analyze security anomalies.

C. Analyze penetration test results.

D. Analyze vulnerability assessments.

Answer: (SHOW ANSWER)

Explanation

Analyzing security anomalies is the most effective way to detect security incidents, as it involves comparing the current state of the information system and network with the expected or normal state, and identifying any deviations or irregularities that may indicate a security breach or compromise. Security anomalies can be detected by using various tools and techniques, such as security information and event management (SIEM) systems, intrusion detection and prevention systems (IDS/IPS), log analysis, network traffic analysis, and behavioral analysis. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4; CISM: Information Security Incident Management Part 11, section recognize security anomalies.

NEW QUESTION: 52

Which of the following is MOST effective in monitoring an organization's existing risk?

A. Periodic updates to risk register

B. Risk management dashboards

C. Security information and event management (SIEM) systems

D. Vulnerability assessment results

Answer: (SHOW ANSWER)

Explanation

Risk management dashboards are the MOST effective in monitoring an organization's existing risk because they provide a visual and interactive representation of the key risk indicators (KRIs) and metrics that reflect the

current risk posture and performance of the organization. Risk management dashboards can help to communicate the risk information to various stakeholders, identify trends and patterns, compare actual results with targets and thresholds, and support decision making and risk response12. Periodic updates to risk register (A) are important to maintain the accuracy and relevance of the risk information, but they are not the most effective in monitoring the existing risk because they do not provide a real-time or dynamic view of the risk situation. Security information and event management (SIEM) systems are effective in monitoring the security events and incidents that may indicate potential or actual threats to the organization, but they are not the most effective in monitoring the existing risk because they do not provide a comprehensive or holistic view of the risk context and impact. Vulnerability assessment results (D) are effective in monitoring the weaknesses and exposures of the organization's assets and systems, but they are not the most effective in monitoring the existing risk because they do not provide a quantitative or qualitative measure of the risk likelihood and consequence. References = 1: CISM Review Manual 15th Edition, page 316-3171; 2: CISM Domain 2: Information Risk Management (IRM) [2022 update]2

NEW QUESTION: 53
Which of the following is MOST critical when creating an incident response plan?
A. Identifying vulnerable data assets
B. Identifying what constitutes an incident
C. Decumenting incident notification and escalation processes
D. Aligning with the risk assessment process
Answer: (SHOW ANSWER)
Explanation
= Documenting incident notification and escalation processes is the most critical step when creating an incident response plan, as this ensures that the appropriate stakeholders are informed and involved in the response process. Identifying vulnerable data assets, what constitutes an incident, and aligning with the risk assessment process are important, but not as critical as documenting the communication and escalation procedures. References = CISM Review Manual 2023, page 1631; CISM Review Questions, Answers & Explanations Manual 2023, page 282

NEW QUESTION: 54
An intrusion has been detected and contained. Which of the following steps represents the BEST practice for ensuring the integrity of the recovered system?
A. Install the OS, patches, and application from the original source.
B. Restore the OS, patches, and application from a backup.
C. Restore the application and data from a forensic copy.
D. Remove all signs of the intrusion from the OS and application.
Answer: (SHOW ANSWER)
Explanation
After an intrusion has been detected and contained, the system should be recovered to a known and trusted state. The best practice for ensuring the integrity of the recovered system is to install the OS, patches, and application from the original source, such as the vendor's website or media. This way, any malicious code or

backdoors that may have been inserted by the intruder can be eliminated. Restoring the OS, patches, and application from a backup may not guarantee the integrity of the system, as the backup may have been compromised or outdated. Restoring the application and data from a forensic copy may preserve the evidence of the intrusion, but it may also reintroduce the vulnerability or malware that allowed the intrusion in the first place. Removing all signs of the intrusion from the OS and application may not be sufficient or feasible, as the intruder may have made subtle or hidden changes that are difficult to detect or undo.
References =
ISACA, CISM Review Manual, 16th Edition, 2020, page 2401
ISACA, CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, 2020, question ID 2132 The BEST practice for ensuring the integrity of the recovered system after an intrusion is to restore the OS, patches, and application from a backup. This will ensure that the system is in a known good state, without any potential residual malicious code or changes from the intrusion. Restoring from a backup also enables the organization to revert to a previous configuration that has been tested and known to be secure. This step should be taken prior to conducting a thorough investigation and forensic analysis to determine the cause and extent of the intrusion.

NEW QUESTION: 55
When management changes the enterprise business strategy which of the following processes should be used to evaluate the existing information security controls as well as to select new information security controls?
A. Configuration management
B. Risk management
C. Access control management
D. Change management
Answer: (SHOW ANSWER)
Explanation
According to the CISM Review Manual (Digital Version), Chapter 3, Section 3.2.2, change management is the process of identifying, assessing, approving, implementing, and monitoring changes to information systems and information security controls1. Change management is essential for ensuring that changes are aligned with the organization's business strategy and objectives, as well as complying with applicable laws and regulations1.
The CISM Review Manual (Digital Version) also states that change management should be performed in conjunction with other processes, such as configuration management, access control management, and risk management1. Configuration management is the process of identifying, documenting, controlling, and verifying the configuration items (CIs) of an information system1. Access control management is the process of granting or denying access to information systems and information assets based on predefined policies and procedures1. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks to information systems and information assets1.
The CISM Exam Content Outline also covers the topic of change management in Domain 3 - Information Security Program Development and Management (27% exam weight)2. The subtopics include:
3.2.2 Change Management
3.2.3 Change Control

3.2.4 Change Implementation
3.2.5 Change Monitoring
I hope this answer helps you prepare for your CISM exam. Good luck!

NEW QUESTION: 56
Which of the following is the PRIMARY benefit of implementing a vulnerability assessment process?
A. Threat management is enhanced.
B. Compliance status is improved.
C. Security metrics are enhanced.
D. Proactive risk management is facilitated.
Answer: (SHOW ANSWER)
Explanation
The primary benefit of implementing a vulnerability assessment process is to facilitate proactive risk management. A vulnerability assessment process is a systematic and periodic evaluation of the security posture of an information system or network, which identifies and measures the weaknesses and exposures that may be exploited by threats. By implementing a vulnerability assessment process, the organization can proactively identify and prioritize the risks, and implement appropriate controls and mitigation strategies to reduce the likelihood and impact of potential incidents. The other options are possible benefits of implementing a vulnerability assessment process, but they are not the primary one. References = CISM Review Manual 15th Edition, page 1731; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 1029

NEW QUESTION: 57
When implementing a security policy for an organization handling personally identifiable information (PII); the MOST important objective should be:
A. strong encryption
B. regulatory compliance.
C. data availability.
D. security awareness training
Answer: (SHOW ANSWER)
Explanation
Regulatory compliance is the most important objective when implementing a security policy for an organization handling personally identifiable information (PII) because it helps to ensure that the organization meets the legal and ethical obligations to protect the privacy and security of PII. PII is any information that can be used to identify, contact, or locate an individual, such as name, address, email, phone number, social security number, etc. PII is subject to various laws and regulations in different jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Failing to comply with these regulations can result in fines, lawsuits, reputational damage, or loss of trust. Therefore, regulatory compliance is the correct answer.
References:

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27018:ed-2:v1:en
https://www.digitalguardian.com/blog/how-secure-personally-identifiable-information-against-loss-or-com
https://blog.rsisecurity.com/how-to-make-a-personally-identifiable-information-policy/

NEW QUESTION: 58
Recommendations for enterprise investment in security technology should be PRIMARILY based on:
A. adherence to international standards
B. availability of financial resources
C. the organization s risk tolerance
D. alignment with business needs
Answer: (SHOW ANSWER)
Explanation
Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1, "Recommendations for enterprise investment in security technology should be primarily based on the organization's risk tolerance."1 Comprehensive and Detailed Explanation: The organization's risk tolerance is the degree of uncertainty that the organization is willing to accept in order to pursue its objectives. It reflects the organization's appetite for risk and its ability to cope with potential losses or disruptions. The higher the risk tolerance, the more aggressive and innovative the security investments can be, as they can help achieve faster growth or competitive advantage. The lower the risk tolerance, the more conservative and defensive the security investments should be, as they can help protect the organization's assets and reputation from potential threats.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.1

NEW QUESTION: 59
An information security manager has been notified about a compromised endpoint device Which of the following is the BEST course of action to prevent further damage?
A. Wipe and reset the endpoint device.
B. Isolate the endpoint device.
C. Power off the endpoint device.
D. Run a virus scan on the endpoint device.
Answer: (SHOW ANSWER)
Explanation
A compromised endpoint device is a potential threat to the security of the network and the data stored on it. The best course of action to prevent further damage is to isolate the endpoint device from the network and other devices, so that the attacker cannot access or spread to other systems. Isolating the endpoint device also allows the information security manager to investigate the incident and determine the root cause, the extent of the compromise, and the appropriate remediation steps. Wiping and resetting the endpoint device may not be feasible or desirable, as it may result in data loss or evidence destruction. Powering off the endpoint device may not stop the attack, as the attacker may have installed persistent malware or backdoors that can resume once the device is powered on again. Running a virus scan on the endpoint device may not be effective, as the attacker may have used sophisticated techniques to evade detection or disable the

antivirus software. References = CISM Review Manual, 15th Edition, page 1741; CISM Review Questions, Answers & Explanations Database, question ID 2112; Using EDR to Address Unmanaged Devices - ISACA3; Boosting Cyberresilience for Critical Enterprise IT Systems With COBIT and NIST Cybersecurity Frameworks - ISACA; Endpoint Security: On the Frontline of Cyber Risk.
The best way to reduce the risk associated with a bring your own device (BYOD) program is to implement a mobile device policy and standard. This policy should include guidelines and rules regarding the use of mobile devices, such as acceptable use guidelines and restrictions on the types of data that can be stored or accessed on the device. Additionally, it should also include requirements for secure mobile device practices, such as the use of strong passwords, encryption, and regular patching. A mobile device management (MDM) solution can also be implemented to help ensure mobile devices meet the organizational security requirements. However, it is not enough to simply implement the policy and MDM solution; employees must also be trained on the secure mobile device practices to ensure the policy is followed.

NEW QUESTION: 60

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized disclosure?

A. Integrity
B. Authenticity
C. Confidentiality
D. Nonrepudiation
Answer: (SHOW ANSWER)
Explanation
Confidentiality is the security objective that best ensures that information is protected against unauthorized disclosure. Confidentiality means that only authorized parties can access or view sensitive or classified information. Integrity means that information is accurate and consistent and has not been tampered with or modified by unauthorized parties. Authenticity means that information is genuine and trustworthy and has not been forged or misrepresented by unauthorized parties. Nonrepudiation means that information can be verified and proven to be sent or received by a specific party without any possibility of denial. References: https://www.csoonline.com/article/3513899/the-cia-triad-definition-components-and-examples.html

NEW QUESTION: 61
Of the following, who is BEST positioned to be accountable for risk acceptance decisions based on risk appetite?
A. Information security manager
B. Chief risk officer (CRO)
C. Information security steering committee
D. Risk owner
Answer: (SHOW ANSWER)
Explanation
The risk owner is the best positioned to be accountable for risk acceptance decisions based on risk appetite, because the risk owner is the person or entity with the accountability and authority to manage a risk1. The risk

owner is responsible for evaluating the risk level, comparing it with the risk appetite, and deciding whether to accept, avoid, transfer, or mitigate the risk2. The risk owner is also accountable for monitoring and reporting on the risk status and outcomes3. The information security manager, the chief risk officer (CRO), and the information security steering committee may have some roles and responsibilities in the risk management process, but they are not the primary accountable parties for risk acceptance decisions.
References = CISM Review Manual, 16th Edition, page 754; Risk Acceptance

NEW QUESTION: 62
Which of the following components of an information security risk assessment is MOST valuable to senior management?
A. Threat profile
B. Residual risk
C. Return on investment (ROI)
D. Mitigation actions
Answer: (SHOW ANSWER)
Explanation
Residual risk is the risk that remains after implementing risk mitigation actions. It is the most valuable component for senior management because it helps them to evaluate the effectiveness and efficiency of risk management and make informed decisions about risk acceptance, transfer or avoidance. References = CISM Review Manual, 16th Edition, Chapter 2, Section 2.3.41

NEW QUESTION: 63
Which of the following would BEST guide the development and maintenance of an information security program?
A. A business impact assessment
B. A comprehensive risk register
C. An established risk assessment process
D. The organization's risk appetite
Answer: (SHOW ANSWER)
Explanation
According to the CISM Manual, the organization's risk appetite is the amount and type of risk that the organization is willing to accept in order to achieve its objectives1. The organization's risk appetite should guide the development and maintenance of an information security program, as it determines the level of

security controls, resources, and activities that are needed to protect the organization's assets and operations1.
The CISM Manual states that "the information security program should be aligned with the organization's risk appetite, which reflects its tolerance for risk and its strategic objectives" (IR 8288A)1. The information security program should also consider other factors that influence the organization's risk appetite, such as its mission, vision, values, culture, stakeholders, regulations, standards, guidelines, and best practices1.
The CISM Manual also provides guidance on how to develop and maintain an information security program based on the organization's risk appetite. It recommends using a process that involves identifying, analyzing, evaluating, treating, monitoring, and reviewing risks that affect the organization's information assets1. It also suggests using a framework or model that supports the development of an information security program based on the organization's risk appetite (e.g., ISO/IEC 27001)1.
References: 1: IR 8288A - Information Security Program Development | CSRC NIST

NEW QUESTION: 64
A forensic examination of a PC is required, but the PC has been switched off. Which of the following should be done FIRST?
A. Perform a backup of the hard drive using backup utilities.
B. Perform a bit-by-bit backup of the hard disk using a write-blocking device
C. Perform a backup of the computer using the network
D. Reboot the system using third-party forensic software in the CD-ROM drive
Answer: (SHOW ANSWER)
Explanation
Performing a bit-by-bit backup of the hard disk using a write-blocking device is the first step to do when a forensic examination of a PC is required, but the PC has been switched off because it helps to create a forensically sound copy of the original evidence without altering or damaging it. A bit-by-bit backup, also known as a physical or raw image, is a complete copy of every bit on the hard disk, including the unallocated or deleted data. A write-blocking device is a hardware or software tool that prevents any write operations to the hard disk, such as updating timestamps or changing file attributes. Performing a bit-by-bit backup of the hard disk using a write-blocking device ensures the integrity and authenticity of the evidence and allows the forensic analysis to be conducted on the duplicate image rather than the original source. Therefore, performing a bit-by-bit backup of the hard disk using a write-blocking device is the correct answer.
References:
https://en.wikipedia.org/wiki/Computer_forensics
https://resources.infosecinstitute.com/topic/computer-forensics-forensic-analysis-examination-planning/
https://www.computer-forensics-recruiter.com/topics/examination_steps/

NEW QUESTION: 65
What is the PRIMARY objective of performing a vulnerability assessment following a business system update?
A. Determine operational losses.
B. Improve the change control process.
C. Update the threat landscape.

D. Review the effectiveness of controls

Answer: (SHOW ANSWER)

Explanation

The primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls. A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1.

A business system update is a process of modifying or enhancing an information system to improve its functionality, performance, security, or compatibility. A business system update may introduce new features, fix bugs, patch vulnerabilities, or comply with new standards or regulations2. Performing a vulnerability assessment following a business system update is important because it helps to:

*Review the effectiveness of controls that are implemented to protect the information sys-tem from threats and risks

*Identify any new or residual vulnerabilities that may have been introduced or exposed by the update

*Evaluate the impact and likelihood of potential incidents that may exploit the vulnerabili-ties

*Prioritize and implement appropriate actions to address the vulnerabilities

*Verify and validate the security posture and compliance of the updated information sys-tem Therefore, the primary objective of performing a vulnerability assessment following a business system update is to review the effectiveness of controls that are designed to ensure the confidentiality, integrity, and availability of the information system and its data. The other options are not the primary objectives of performing a vulnerability as-sessment following a business system update. Determining operational losses is not an objective, but rather a possible consequence of not performing a vulnerability as-sessment or not addressing the identified vulnerabilities. Improving the change control process is not an objective, but rather a possible outcome of performing a vulnerability assessment and incorporating its results and recommendations into the change man-agement cycle. Updating the threat landscape is not an objective, but rather a prereq-uisite for performing a vulnerability assessment that requires using up-to-date sources of threat intelligence and vulnerability information. References: 1: Vulnerability As-sessment - NIST 2: System Update - Techopedia : Vulnerability Assessment vs Penetra-tion Testing - Imperva : Change Control Process - NIST : Threat Landscape - NIST

NEW QUESTION: 66

A business requires a legacy version of an application to operate but the application cannot be patched. To limit the risk exposure to the business, a firewall is implemented in front of the legacy application. Which risk treatment option has been applied?

A. Mitigate

B. Accept

C. Transfer

D. Avoid

Answer: (SHOW ANSWER)

Explanation

Mitigate is the risk treatment option that has been applied by implementing a firewall in front of the legacy application because it helps to reduce the impact or probability of a risk. Mitigate is a process of taking actions to lessen the negative effects of a risk, such as implementing security controls, policies, or procedures. A firewall is a security device that monitors and filters the network traffic between the legacy application and the external network, blocking or allowing packets based on predefined rules. A firewall helps to mitigate the risk of unauthorized access, exploitation, or attack on the legacy application that cannot be patched. Therefore, mitigate is the correct answer.
References:
https://simplicable.com/risk/risk-treatment
https://resources.infosecinstitute.com/topic/risk-treatment-options-planning-prevention/
https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-process/

NEW QUESTION: 67
Which of the following is the MOST important reason for obtaining input from risk owners when implementing controls?
A. To reduce risk mitigation costs
B. To resolve vulnerabilities in enterprise architecture (EA)
C. To manage the risk to an acceptable level
D. To eliminate threats impacting the business
Answer: (SHOW ANSWER)
Explanation
According to the Certified Information Security Manager (CISM) Study Manual, risk owners are responsible for managing a risk, including taking corrective action to reduce the risk to an acceptable level. When implementing controls, it is essential to obtain input from risk owners to ensure that the controls are effective in managing the risk to an acceptable level.
By obtaining input from risk owners, the organization can ensure that the controls are tailored to the specific risks and are effective in reducing the risk to an acceptable level. This can help to minimize the impact of the risk on the organization and reduce the potential for financial or reputational damage.

NEW QUESTION: 68
Which of the following is MOST important to consider when aligning a security awareness program with the organization's business strategy?
A. Regulations and standards
B. People and culture
C. Executive and board directives
D. Processes and technology
Answer: (SHOW ANSWER)
Explanation
A security awareness program is a set of activities designed to educate and motivate employees to adopt secure behaviors and practices. A security awareness program should be aligned with the organization's business strategy, which defines the vision, mission, goals and objectives of the organization. The most

important factor to consider when aligning a security awareness program with the business strategy is the people and culture of the organization, because they are the primary target audience and the key enablers of the program. The people and culture of the organization influence the level of awareness, the attitude and the behavior of the employees towards information security. Therefore, a security awareness program should be tailored to the specific needs, preferences, values and expectations of the people and culture of the organization, and should use appropriate methods, channels, messages and incentives to engage and influence them. A security awareness program that is aligned with the people and culture of the organization will have a higher chance of achieving its objectives and improving the overall security posture of the organization.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: Information Security & Business Process Alignment, video 22

NEW QUESTION: 69
The PRIMARY reason for creating a business case when proposing an information security project is to:
A. articulate inherent risks.
B. provide demonstrated return on investment (ROI).
C. establish the value of the project in relation to business objectives.
D. gain key business stakeholder engagement.
Answer: (SHOW ANSWER)
Explanation
The primary reason for creating a business case when proposing an information security project is to establish the value of the project in relation to the business objectives and to justify the investment required. A business case should demonstrate how the project aligns with the organization's strategy, goals, and mission, and how it supports the business processes and functions. A business case should also include the expected benefits, costs, risks, and alternatives of the project, and provide a clear rationale for choosing the preferred option.
References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 70
Which of the following presents the GREATEST risk associated with the use of an automated security information and event management (SIEM) system?

A. Low number of false positives
B. Low number of false negatives
C. High number of false positives
D. High number of false negatives
Answer: (SHOW ANSWER)
Explanation
A false negative is a security incident that was not detected by the SIEM system, which presents the greatest risk as it allows attackers to compromise the organization's assets and data without being noticed or stopped.

A high number of false negatives can indicate that the SIEM system is not configured properly, has insufficient data sources, or lacks effective analytics and correlation rules. (From CISM Review Manual 15th Edition)
References: CISM Review Manual 15th Edition, page 181, section 4.3.2.4.

NEW QUESTION: 71
Before approving the implementation of a new security solution, senior management requires a business case. Which of the following would BEST support the justification for investment?
A. The solution contributes to business strategy.
B. The solution improves business risk tolerance levels.
C. The solution improves business resiliency.
D. The solution reduces the cost of noncompliance with regulations.
Answer: (SHOW ANSWER)
Explanation
The best way to support the justification for investment in a new security solution is to show how the solution contributes to the business strategy of the organization. The business strategy defines the vision, mission, goals, and objectives of the organization, and the security solution should align with and support them. The security solution should also demonstrate how it adds value to the organization, such as by enabling new business opportunities, enhancing customer satisfaction, or increasing competitive advantage. The business case should include the expected benefits, costs, risks, and alternatives of the security solution, and provide a clear rationale for choosing the preferred option1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 1: Information Security Governance, Section: Information Security Strategy, Subsection: Business Case Development, Page 33.

NEW QUESTION: 72
Which of the following is the MOST important consideration when updating procedures for managing security devices?
A. Updates based on the organization's security framework
B. Notification to management of the procedural changes
C. Updates based on changes m risk technology and process
D. Review and approval of procedures by management
Answer: (SHOW ANSWER)
Explanation
According to the CISM Manual, updating procedures for managing security devices should be based on changes in risk technology and process, not on the organization's security framework, notification to management of the procedural changes, or review and approval of procedures by management1. These are not the most important considerations when updating procedures for managing security devices, as they do not reflect the actual impact of the changes on the security posture of the organization.
The CISM Manual states that "procedures for managing security devices should be updated whenever there are significant changes in the risk technology or process that affect the security devices" (IR 8287A)1. For example, if a new security device is introduced or an existing one is replaced, its procedures should be

updated accordingly. Similarly, if a new risk technology or process is implemented that affects how security devices are configured, monitored, or maintained, its procedures should be updated as well1.
The CISM Manual also provides guidance on how to update procedures for managing security devices in a systematic and consistent manner. It recommends using a change management process that involves identifying, analyzing, approving, implementing, and evaluating changes to security device procedures1. It also suggests using a change control board (CCB) that consists of representatives from different stakeholders who review and approve changes to security device procedures before they are implemented1.
References: 1: IR 8287A - Managing Security Devices | CSRC NIST

NEW QUESTION: 73
Which of the following is the PRIMARY benefit achieved when an information security governance framework is aligned with corporate governance?
A. Protection of business value and assets
B. Identification of core business strategies
C, Easier entrance into new businesses and technologies
C. Improved regulatory compliance posture
Answer: (SHOW ANSWER)
Explanation
Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are effectively managed. By aligning information security governance with corporate governance, the organization can ensure that information security is integrated into the business processes and decision making, and that the information security risks and opportunities are properly identified, assessed, and addressed. References = CISM Review Manual, 16th Edition, Chapter 1, Section 1.1

NEW QUESTION: 74
Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?
A. Existence of a right-to-audit clause
B. Results of the provider's business continuity tests
C. Technical capabilities of the provider
D. Existence of the provider's incident response plan
Answer: (SHOW ANSWER)
Explanation
The technical capabilities of the provider are the MOST important thing for an information security manager to verify when selecting a third-party forensics provider because they determine the quality, reliability, and validity of the forensic services and results that the provider can deliver. The technical capabilities of the provider include the skills, experience, and qualifications of the forensic staff, the methods, tools, and standards that the forensic staff use, and the facilities, equipment, and resources that the forensic staff have. The information security manager should verify that the technical capabilities of the provider match the forensic needs and expectations of the organization, such as the type, scope, and complexity of the forensic investigation, the

legal and regulatory requirements, and the time and cost constraints12. The existence of a right-to-audit clause (A) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. A right-to-audit clause is a contractual provision that grants the organization the right to audit or review the performance, compliance, and security of the provider. A right-to-audit clause can help to ensure the accountability, transparency, and quality of the provider, as well as to identify and resolve any issues or disputes that may arise during or after the forensic service. However, a right-to-audit clause does not guarantee that the provider has the technical capabilities to conduct the forensic service effectively and efficiently12. The results of the provider's business continuity tests (B) are an important thing for an information security manager to verify when selecting a third-party forensics provider, but they are not the MOST important thing. The results of the provider's business continuity tests can indicate the ability and readiness of the provider to continue or resume the forensic service in the event of a disruption, disaster, or emergency. The results of the provider's business continuity tests can help to assess the availability, resilience, and recovery of the provider, as well as to mitigate the risks of losing or compromising the forensic evidence or data. However, the results of the provider's business continuity tests do not ensure that the provider has the technical capabilities to perform the forensic service accurately and professionally12. The existence of the provider's incident response plan (D) is an important thing for an information security manager to verify when selecting a third-party forensics provider, but it is not the MOST important thing. The existence of the provider's incident response plan can demonstrate the preparedness and capability of the provider to detect, report, and respond to any security incidents that may affect the forensic service or the organization. The existence of the provider's incident response plan can help to protect the confidentiality, integrity, and availability of the forensic evidence or data, as well as to comply with the legal and contractual obligations. However, the existence of the provider's incident response plan does not confirm that the provider has the technical capabilities to execute the forensic service competently and ethically12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance - ISACA2

NEW QUESTION: 75

A security incident has been reported within an organization. When should an information security manager contact the information owner?

A. After the incident has been contained

B. After the incident has been mitigated

C. After the incident has been confirmed

D. After the potential incident has been logged

Answer: (SHOW ANSWER)

Explanation

The information owner is the person who has the authority and responsibility for the information asset and its protection. The information security manager should contact the information owner as soon as possible after the incident has been confirmed, to inform them of the incident, its impact, and the actions taken or planned to resolve it. The information owner may also need to be involved in the decision-making process regarding the incident response and recovery. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 76
A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?
A. Right of the subscriber to conduct onsite audits of the vendor
B. Escrow of software code with conditions for code release
C. Authority of the subscriber to approve access to its data
D. Commingling of subscribers' data on the same physical server
Answer: (SHOW ANSWER)
Explanation
The greatest concern to an information security manager if omitted from the contract with a multinational cloud computing vendor would be the authority of the subscriber to approve access to its data. This is because the subscriber's data may be subject to different legal and regulatory requirements in different jurisdictions, and the subscriber may lose control over who can access, process, or disclose its data. The subscriber should have the right to approve or deny access to its data by the vendor or any third parties, and to ensure that the vendor complies with the applicable data protection laws and standards. The authority of the subscriber to approve access to its data is also one of the key elements of the ISACA Cloud Computing Management Audit/Assurance Program1.
References = CISM Review Manual, 16th Edition eBook2, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 142.

NEW QUESTION: 77
The business value of an information asset is derived from:
A. the threat profile.
B. its criticality.
C. the risk assessment.
D. its replacement cost.
Answer: (SHOW ANSWER)
Explanation
The business value of an information asset is derived from its criticality, which is the degree of importance or dependency of the asset to the organization's objectives, operations, and stakeholders. The criticality of an information asset can be determined by assessing its impact on the confidentiality, integrity, and availability

(CIA) of the information, as well as its sensitivity, classification, and regulatory requirements. The higher the criticality of an information asset, the higher its business value, and the more resources and controls are needed to protect it.
References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; IT Asset Valuation, Risk Assessment and Control Implementation Model1; Managing Data as an Asset3

NEW QUESTION: 78
Which of the following should an information security manager do FIRST when creating an organization's disaster recovery plan (DRP)?
A. Conduct a business impact analysis (BIA)
B. Identify the response and recovery learns.
C. Review the communications plan.
D. Develop response and recovery strategies.
Answer: (SHOW ANSWER)
Explanation
Conducting a business impact analysis (BIA) is the first step when creating an organization's disaster recovery plan (DRP) because it helps to identify and prioritize the critical business functions or processes that need to be restored after a disruption, and determine their recovery time objectives (RTOs) and recovery point objectives (RPOs)2. Identifying the response and recovery teams is not the first step, but rather a subsequent step that involves assigning roles and responsibilities for executing the DRP. Reviewing the communications plan is not the first step, but rather a subsequent step that involves defining the communication channels and protocols for notifying and updating the stakeholders during and after a disruption. Developing response and recovery strategies is not the first step, but rather a subsequent step that involves selecting and implementing the appropriate solutions and procedures for restoring the critical business functions or processes. References: 2
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/business-impact-analysis-bia-and-disaster-r

NEW QUESTION: 79
An employee of an organization has reported losing a smartphone that contains sensitive information The BEST step to address this situation is to:
A. disable the user's access to corporate resources.
B. terminate the device connectivity.
C. remotely wipe the device
D. escalate to the user's management
Answer: (SHOW ANSWER)
Explanation
The best step to address the situation of losing a smartphone that contains sensitive information is to remotely wipe the device, which means erasing all the data on the device and restoring it to factory settings. Remotely wiping the device can prevent unauthorized access to the sensitive information and protect the organization from data breaches or leaks. Remotely wiping the device can be done through services such as Find My

Device for Android or Find My iPhone for iOS, or through mobile device management (MDM) solutions. The other options, such as disabling the user's access, terminating the device connectivity, or escalating to the user's management, may not be effective or timely enough to secure the sensitive information on the device.
References:
https://www.security.org/resources/protect-data-lost-device/
https://support.google.com/android/answer/6160491?hl=en
https://www.pcmag.com/how-to/locate-lock-erase-how-to-find-lost-android-phone

NEW QUESTION: 80

Which of the following is the GREATEST concern resulting from the lack of severity criteria in incident classification?

A. Statistical reports will be incorrect.
B. The service desk will be staffed incorrectly.
C. Escalation procedures will be ineffective.
D. Timely detection of attacks will be impossible.
Answer: (SHOW ANSWER)
Explanation
The greatest concern resulting from the lack of severity criteria in incident classification is that escalation procedures will be ineffective because they rely on severity criteria to determine when and how to escalate an incident to higher levels of authority or responsibility, and what actions or resources are required for resolving an incident. Statistical reports will be incorrect is not a great concern because they do not affect the incident response process directly, but rather provide information or analysis for improvement or evaluation purposes. The service desk will be staffed incorrectly is not a great concern because it does not affect the incident response process directly, but rather affects the availability or efficiency of one of its components. Timely detection of attacks will be impossible is not a great concern because it does not depend on severity criteria, but rather on monitoring and alerting mechanisms. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 81
Which of the following would provide the BEST input to a business case for a technical solution to address potential system vulnerabilities?
A. Risk assessment
B. Business impact analysis (BIA)
C. Penetration test results
D. Vulnerability scan results
Answer: (SHOW ANSWER)
Explanation
Risk assessment is the BEST input to a business case for a technical solution to address potential system vulnerabilities, because it helps to identify and prioritize the most critical risks that the solution should mitigate

or reduce. Risk assessment also helps to evaluate the costs and benefits of the solution in terms of reducing the likelihood and impact of potential threats and incidents.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 47: "Risk assessment is the process of identifying and analyzing information security risks and determining their potential impact on the enterprise's business objectives." CISM Review Manual, 16th Edition, ISACA, 2020, p. 48: "Risk assessment provides input to the business case for information security investments by identifying and prioritizing the most critical risks that need to be addressed and evaluating the costs and benefits of the proposed solutions."

NEW QUESTION: 82
Which of the following is the BEST starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities?
A. Controls analysis
B. Emerging risk review
C. Penetration testing
D. Traffic monitoring
Answer: (SHOW ANSWER)
Explanation
The best starting point for a newly hired information security manager who has been tasked with identifying and addressing network vulnerabilities is C. Penetration testing. This is because penetration testing is a method of simulating real-world attacks on a network to evaluate its security posture and identify any weaknesses or gaps that could be exploited by malicious actors. Penetration testing can help the information security manager to assess the effectiveness of the existing controls, prioritize the remediation efforts, and demonstrate compliance with the relevant standards and regulations. Penetration testing can also provide valuable insights into the network architecture, configuration, and behavior, as well as the potential impact and likelihood of different types of attacks.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 50, page 14

NEW QUESTION: 83
What should be an information security manager's MOST important consideration when developing a multi-year plan?
A. Ensuring contingency plans are in place for potential information security risks
B. Ensuring alignment with the plans of other business units
C. Allowing the information security program to expand its capabilities
D. Demonstrating projected budget increases year after year
Answer: (SHOW ANSWER)
Explanation
= The most important consideration when developing a multi-year plan for information security is to ensure alignment with the plans of other business units. Alignment means that the information security plan supports and enables the achievement of the business objectives, strategies, and priorities of the organization and its

various units. Alignment also means that the information security plan is consistent and compatible with the plans of other business units, and that it addresses the needs, expectations, and requirements of the relevant stakeholders1 .

By ensuring alignment with the plans of other business units, the information security manager can achieve the following benefits1 :

Increase the value and effectiveness of information security: By aligning the information security plan with the business goals and drivers, the information security manager can demonstrate the value and contribution of information security to the organization's performance, growth, and competitiveness.

The information security manager can also ensure that the information security plan addresses the most critical and relevant risks and opportunities for the organization and its units, and that it provides adequate and appropriate protection and support for the organization's assets, processes, and activities.

Enhance the communication and collaboration with other business units: By aligning the information security plan with the plans of other business units, the information security manager can enhance the communication and collaboration with the other business unit leaders and managers, who are the key stakeholders and partners in information security. The information security manager can also solicit and incorporate their input, feedback, and suggestions into the information security plan, and provide them with timely and relevant information, guidance, and support. The information security manager can also foster a culture of trust, respect, and cooperation among the different business units, and promote a shared vision and commitment to information security.

Optimize the use and allocation of resources for information security: By aligning the information security plan with the plans of other business units, the information security manager can optimize the use and allocation of resources for information security, such as budget, staff, time, or technology. The information security manager can also avoid duplication, conflict, or waste of resources among the different business units, and ensure that the information security plan is feasible, realistic, and sustainable. The information security manager can also leverage the resources and capabilities of other business units to enhance the information security plan, and provide them with the necessary resources and capabilities to implement and maintain the information security plan.

The other options are not the most important consideration when developing a multi-year plan for information security, as they are less strategic, comprehensive, or impactful than ensuring alignment with the plans of other business units. Ensuring contingency plans are in place for potential information security risks is an important component of the information security plan, but it is not the most important consideration, as it focuses on the reactive and preventive aspects of information security, rather than the proactive and enabling aspects.

Allowing the information security program to expand its capabilities is an important objective of the information security plan, but it is not the most important consideration, as it depends on the availability and suitability of the resources, technologies, and opportunities for information security, and it may not align with the organization's needs, priorities, or constraints. Demonstrating projected budget increases year after year is an important outcome of the information security plan, but it is not the most important consideration, as it reflects the cost and demand of information security, rather than the value and benefit of information security, and it may not be justified or supported by the organization's financial situation or expectations1 . References = CISM Domain 1: Information Security Governance (ISG) [2022 update], CISM Domain 2: Information Risk

Management (IRM) [2022 update], Aligning Information Security with Business Strategy - ISACA, [Aligning Information Security with Business Objectives - ISACA]

NEW QUESTION: 84
An organization is aligning its incident response capability with a public cloud service provider. What should be the information security manager's FIRST course of action?
A. Identify the skill set of the provider's incident response team.
B. Evaluate the provider's audit logging and monitoring controls.
C. Review the provider's incident definitions and notification criteria.
D. Update the incident escalation process.
Answer: (SHOW ANSWER)
Explanation
When an organization is aligning its incident response capability with a public cloud service provider, the information security manager's first course of action should be to review the provider's incident definitions and notification criteria. This is because the provider's incident definitions and notification criteria may differ from the organization's own, and may affect the scope, severity, and urgency of the incidents that need to be reported and handled. By reviewing the provider's incident definitions and notification criteria, the information security manager can ensure that there is a common understanding and agreement on what constitutes an incident, how it is classified, and when and how it is communicated. This will help to avoid confusion, delays, or conflicts in the incident response process, and to establish clear roles and responsibilities between the organization and the provider. References = CISM Review Manual, 16th Edition, page 1021 Reviewing the provider's incident definitions and notification criteria is the FIRST course of action when aligning the organization's incident response capability with a public cloud service provider. This is because the organization needs to understand how the provider defines and classifies incidents, what their roles and responsibilities are, and how they will communicate with the organization in case of an incident. This will help the organization align its own incident response processes and expectations with the provider's and ensure a coordinated and effective response.

NEW QUESTION: 85
To improve the efficiency of the development of a new software application, security requirements should be defined:
A. based on code review.
B. based on available security assessment tools.
C. after functional requirements.
D. concurrently with other requirements.
Answer: (SHOW ANSWER)
Explanation
Security requirements should be defined concurrently with other requirements to ensure that security is built into the software development process from the beginning and not added as an afterthought. This will also improve the efficiency of the development process by reducing the need for rework and testing. Security requirements should be based on the business objectives, risk assessment, and security policies of the

organization, not on code review, security assessment tools, or functional requirements. References = CISM Review Manual 15th Edition, page 1241; CISM Item Development Guide, page 62

NEW QUESTION: 86
Which of the following is the PRIMARY benefit of implementing an information security governance framework?
A. The framework defines managerial responsibilities for risk impacts to business goals.
B. The framework provides direction to meet business goals while balancing risks and controls.
C. The framework provides a roadmap to maximize revenue through the secure use of technology.
D. The framework is able to confirm the validity of business goals and strategies.
Answer: (SHOW ANSWER)
Explanation
An information security governance framework is a set of principles, policies, standards, and processes that guide the development, implementation, and management of an effective information security program that supports the organization's objectives and strategy. The framework provides direction to meet business goals while balancing risks and controls, as it helps to align the information security activities with the business needs, priorities, and risk appetite, and to ensure that the security resources and investments are optimized and justified.
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 87
Which of the following MUST be established to maintain an effective information security governance framework?
A. Security controls automation
B. Defined security metrics
C. Change management processes
D. Security policy provisions
Answer: (SHOW ANSWER)
Explanation
Security policy provisions are the statements or rules that define the information security objectives, principles, roles and responsibilities, and requirements for the organization. Security policy provisions must be established to maintain an effective information security governance framework, as they provide the foundation and direction for the information security activities and processes within the organization. Security policy provisions also help to align the information security governance framework with the business strategy and objectives, and ensure compliance with relevant laws and regulations. The other options, such as security controls automation, defined security metrics, or change management processes, are important components of an information security governance framework, but they are not essential to establish it. References:
https://www.iso.org/standard/74046.html
https://www.nistf.gov/cyberframework
https://www.iso.org/standard/27001

NEW QUESTION: 88
Recovery time objectives (RTOs) are an output of which of the following?
A. Business continuity plan (BCP)
B. Disaster recovery plan (DRP)
C. Service level agreement (SLA)
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
Explanation
Business impact analysis (BIA) is the process that provides the output of recovery time objectives (RTOs), which are the maximum acceptable time frames for restoring business functions or processes after a disruption. Business continuity plan (BCP) is the document that describes the strategies and procedures for ensuring the continuity of critical business functions or processes in the event of a disruption. Disaster recovery plan (DRP) is the document that describes the technical steps and resources for restoring IT systems and data in the event of a disruption. Service level agreement (SLA) is the document that defines the expectations and obligations between a service provider and a service consumer, such as availability, performance, and security. References:
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/business-impact-analysis-bia-and-disaster-re
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/service-level-agreements-in-the-cloud

NEW QUESTION: 89
Measuring which of the following is the MOST accurate way to determine the alignment of an information security strategy with organizational goals?
A. Number of blocked intrusion attempts
B. Number of business cases reviewed by senior management
C. Trends in the number of identified threats to the business
D. Percentage of controls integrated into business processes
Answer: (SHOW ANSWER)
Explanation
Measuring the percentage of controls integrated into business processes is the most accurate way to determine the alignment of an information security strategy with organizational goals, as this reflects the extent to which the information security program supports and enables the business objectives and activities, and reduces the friction and resistance from the business stakeholders. The percentage of controls integrated into business processes also indicates the maturity and effectiveness of the information security program, and the level of awareness and acceptance of the information security policies and standards among the business users. Number of blocked intrusion attempts, number of business cases reviewed by senior management, and trends in the number of identified threats to the business are not the most accurate ways to determine the alignment of an information security strategy with organizational goals, as they do not measure the impact and value of the information security program on the business performance and outcomes, and may not reflect the business priorities and expectations. References = CISM Review Manual 2023, page 291; CISM Review

Questions, Answers & Explanations Manual 2023, page 372; ISACA CISM - iSecPrep, page 223; CISM Exam Overview - Vinsys4

NEW QUESTION: 90

Which of the following is MOST important to include in an information security status report to senior management?

A. Key risk indicators (KRIs)

B. Review of information security policies

C. Information security budget requests

D. List of recent security events

Answer: (SHOW ANSWER)

Explanation

According to the CISM Review Manual, key risk indicators (KRIs) are the most important information to include in an information security status report to senior management, as they provide a measure of the current level of risk exposure and the effectiveness of the risk management activities. KRIs also help to identify trends, patterns and emerging risks that may require management attention or action.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 209

NEW QUESTION: 91

Which of the following BEST supports information security management in the event of organizational changes in security personnel?

A. Formalizing a security strategy and program

B. Developing an awareness program for staff

C. Ensuring current documentation of security processes

D. Establishing processes within the security operations team

Answer: (SHOW ANSWER)

Explanation

Ensuring current documentation of security processes is the best way to support information security management in the event of organizational changes in security personnel. Documentation of security processes provides a clear and consistent reference for the roles, responsibilities, procedures, and standards of the information security program. It helps to maintain the continuity and effectiveness of the security operations, as well as the compliance with the security policies and regulations. Documentation of security processes also facilitates the knowledge transfer and training of new or existing security personnel, as well as the communication and collaboration with other stakeholders. By ensuring current documentation of security processes, the information security manager can minimize the impact of organizational changes in security personnel, and ensure a smooth transition and alignment of the security program. References = CISM Review Manual 15th Edition, page 43, page 45.

NEW QUESTION: 92
Which of the following BEST helps to ensure a risk response plan will be developed and executed in a timely manner?
A. Establishing risk metrics
B. Training on risk management procedures
C. Reporting on documented deficiencies
D. Assigning a risk owner
Answer: (SHOW ANSWER)
Explanation
Assigning a risk owner is the best way to ensure a risk response plan will be developed and executed in a timely manner, because a risk owner is responsible for monitoring, controlling, and reporting on the risk, as well as implementing the appropriate risk response actions. A risk owner should have the authority, accountability, and resources to manage the risk effectively. Establishing risk metrics, training on risk management procedures, and reporting on documented deficiencies are all important aspects of risk management, but they do not guarantee that a risk response plan will be executed promptly and properly. Risk metrics help to measure and communicate the risk level and performance, but they do not assign any responsibility or action. Training on risk management procedures helps to increase the awareness and competence of the staff involved in risk management, but it does not ensure that they will follow the procedures or have the authority to do so. Reporting on documented deficiencies helps to identify and communicate the gaps and weaknesses in the risk management process, but it does not provide any solutions or corrective actions. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 125-126,
136-137.

NEW QUESTION: 93
Which of the following is the BEST course of action when an online company discovers a network attack in progress?
A. Dump all event logs to removable media
B. Isolate the affected network segment
C. Enable trace logging on ail events
D. Shut off all network access points
Answer: (SHOW ANSWER)
Explanation
The BEST course of action when an online company discovers a network attack in progress is to isolate the affected network segment. This prevents the attacker from gaining further access to the network and limits the

scope of the attack. Dumping event logs to removable media and enabling trace logging may be useful for forensic purposes, but should not be the first course of action in the midst of an active attack. Shutting off all network access points would be too drastic and would prevent legitimate traffic from accessing the network.

NEW QUESTION: 94
An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance.
Which of the following would provide the MOST useful information for planning purposes?
A. Results from a business impact analysis (BIA)
B. Deadlines and penalties for noncompliance
C. Results from a gap analysis
D. An inventory of security controls currently in place
Answer: (SHOW ANSWER)
Explanation
Results from a gap analysis would provide the most useful information for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. A gap analysis is an assessment of the difference between an organization's current state of compliance and its desired level or standard. It is a process used to identify potential areas for improvement by comparing actual performance with expected performance. A gap analysis can help to prioritize the actions needed to close the gaps and comply with the regulatory requirements, as well as to estimate the resources and time required for each action1. The other options are not as useful as results from a gap analysis for planning purposes when preparing an action plan to achieve compliance with local regulatory requirements by an established deadline. Deadlines and penalties for noncompliance are important factors to consider, but they do not provide information on how to achieve compliance or what actions are needed2. Results from a business impact analysis (BIA) are useful for identifying the critical processes and assets that need to be protected, but they do not provide information on how to comply with the regulatory requirements or what actions are needed3. An inventory of security controls currently in place is useful for assessing the current state of compliance, but it does not provide information on how to comply with the regulatory requirements or what actions are needed4.
References: 3: Business impact analysis (BIA) - Wikipedia 2: Compliance Gap Analysis & Effectiveness Evaluation | SMS 1: What is Gap Analysis in Compliance | Scytale 4: Gap Analysis & Risk Assessment - Riddle Compliance

NEW QUESTION: 95
An organization's quality process can BEST support security management by providing:
A. security configuration controls.
B. assurance that security requirements are met.
C. guidance for security strategy.
D. a repository for security systems documentation.
Answer: (SHOW ANSWER)
Explanation

= A quality process is a set of activities that ensures that the products or services delivered by an organization meet the customer's expectations and comply with the applicable standards and regulations. A quality process can support security management by providing assurance that security requirements are met throughout the development, implementation and maintenance of information systems and processes. A quality process can also help to identify and correct security defects, measure security performance and effectiveness, and improve security practices and procedures. References = CISM Review Manual, 15th Edition, page 671; CISM Review Questions, Answers & Explanations Database, question ID 2092.
An organization's quality process can BEST support security management by providing assurance that security requirements are met. This means that the quality process can be used to ensure that security controls are being implemented as intended and that they are achieving the desired results. This helps to ensure that the organization is properly protected and that it is in compliance with security regulations and standards.

NEW QUESTION: 96
When developing a categorization method for security incidents, the categories MUST:
A. align with industry standards.
B. be created by the incident handler.
C. have agreed-upon definitions.
D. align with reporting requirements.
Answer: C (LEAVE A REPLY)
Explanation
When developing a categorization method for security incidents, the categories must have agreed-upon definitions. This means that the categories should be clear, consistent, and understandable for all the parties involved in the incident response process, such as the incident handlers, the stakeholders, the management, and the external authorities. Having agreed-upon definitions for the categories can help to ensure that the incidents are classified and reported accurately, that the appropriate actions and resources are allocated, and that the communication and coordination are effective. Aligning with industry standards, creating by the incident handler, and aligning with reporting requirements are not mandatory for developing a categorization method for security incidents, although they may be desirable or beneficial depending on the context and objectives of the organization. Aligning with industry standards can help to adopt best practices and benchmarks for incident response, but it may not be feasible or suitable for all types of incidents or organizations. Creating by the incident handler can allow for flexibility and customization of the categories, but it may also introduce inconsistency and ambiguity if the definitions are not shared or agreed upon by others. Aligning with reporting requirements can help to comply with legal or contractual obligations, but it may not cover all the aspects or dimensions of the incidents that need to be categorized. References = CISM Review Manual, 16th Edition, pages 200-2011; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 822 When developing a categorization method for security incidents, the categories MUST have agreed-upon definitions. This is because having clear and consistent definitions for each category of incidents will help to ensure a common understanding and communication among the incident response team and other stakeholders. It will also facilitate the accurate and timely identification, classification, reporting and analysis of incidents. Having agreed-upon definitions will also help to avoid confusion, ambiguity and inconsistency in the incident management process

NEW QUESTION: 97
An organization's HR department requires that employee account privileges be removed from all corporate IT systems within three days of termination to comply with a government regulation However, the systems all have different user directories, and it currently takes up to four weeks to remove the privileges Which of the following would BEST enable regulatory compliance?
A. Multi-factor authentication (MFA) system
B. Identity and access management (IAM) system
C. Privileged access management (PAM) system
D. Governance, risk, and compliance (GRC) system
Answer: (SHOW ANSWER)
Explanation
= An identity and access management (IAM) system is a set of processes, policies, and technologies that enable an organization to manage the identities and access rights of its users across different systems and applications1. An IAM system can help an organization to comply with the government regulation by automating the provisioning and deprovisioning of user accounts, enforcing consistent access policies, and integrating different user directories2. An IAM system can also provide audit trails and reports to demonstrate compliance with the regulation3. A multi-factor authentication (MFA) system is a method of verifying the identity of a user by requiring two or more factors, such as something the user knows, has, or is4. An MFA system can enhance the security of user authentication, but it does not address the issue of removing user privileges from different systems within three days of termination. A privileged access management (PAM) system is a solution that manages and monitors the access of privileged users, such as administrators, to critical systems and resources. A PAM system can reduce the risk of unauthorized or malicious use of privileged accounts, but it does not solve the problem of managing the access of regular users across different systems. A governance, risk, and compliance (GRC) system is a software platform that integrates the functions of governance, risk management, and compliance management. A GRC system can help an organization to align its objectives, policies, and processes with the relevant regulations, standards, and best practices, but it does not directly enable the removal of user privileges from different systems within three days of termination.
References = 1: CISM Review Manual (Digital Version), page 24 2: 1 3: 2 4: CISM Review Manual (Digital Version), page 25 : CISM Review Manual (Digital Version), page 26 : CISM Review Manual (Digital Version), page 27

NEW QUESTION: 98
Which of the following is MOST appropriate to communicate to senior management regarding information risk?
A. Defined risk appetite
B. Emerging security technologies
C. Vulnerability scanning progress
D. Risk profile changes
Answer: (SHOW ANSWER)
Explanation

The most appropriate information to communicate to senior management regarding information risk is the risk profile changes, which reflect the current level and nature of the risks that the organization faces. The risk profile changes can help senior management to understand the impact of the risks on the business objectives, the effectiveness of the risk management strategy, and the need for any adjustments or improvements. The risk profile changes can also help senior management to prioritize the allocation of resources and to make informed decisions.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Communication, Subsection: Risk Reporting, Page 97.

NEW QUESTION: 99
Which of the following is MOST important to consider when defining control objectives?
A. Industry best practices
B. An information security framework
C. Control recommendations from a recent audit
D. The organization's risk appetite
Answer: (SHOW ANSWER)
Explanation
The organization's risk appetite is the most important factor to consider when defining control objectives, because it reflects the amount and type of risk that the organization is willing to accept or avoid in pursuit of its goals. Control objectives should align with the risk appetite and support the achievement of the organization's objectives. Industry best practices, an information security framework, and control recommendations from a recent audit are also useful sources of guidance, but they are not as critical as the risk appetite.
References = CISM Review Manual, 16th Edition, page 75

NEW QUESTION: 100
Which of the following is the MOST effective way to convey information security responsibilities across an organization?

A. Implementing security awareness programs
B. Documenting information security responsibilities within job descriptions
C. Developing a skills matrix
D. Defining information security responsibilities in the security policy
Answer: (SHOW ANSWER)
Explanation
Documenting information security responsibilities within job descriptions is the most effective way to convey information security responsibilities across an organization because it clearly defines the roles, expectations, and accountabilities of each employee regarding information security. It also helps to align the information security objectives with the business goals and performance indicators, and to ensure compliance with the security policies and standards.
References = CISM Review Manual 15th Edition, What is CISM? - Digital Guardian

NEW QUESTION: 101

Which of the following is the BEST approach for governing noncompliance with security requirements?
A. Base mandatory review and exception approvals on residual risk,
B. Require users to acknowledge the acceptable use policy.
C. Require the steering committee to review exception requests.
D. Base mandatory review and exception approvals on inherent risk.
Answer: (SHOW ANSWER)
Explanation
= Residual risk is the risk that remains after applying security controls. It reflects the actual exposure of the organization to noncompliance issues. Therefore, basing mandatory review and exception approvals on residual risk is the best approach for governing noncompliance with security requirements. It ensures that the organization is aware of the potential impact and likelihood of noncompliance and can make informed decisions about accepting, mitigating, or transferring the risk. References = CISM Review Manual 15th Edition, page 78.

NEW QUESTION: 102
Regular vulnerability scanning on an organization's internal network has identified that many user workstations have unpatched versions of software. What is the BEST way for the information security manager to help senior management understand the related risk?
A. Include the impact of the risk as part of regular metrics.
B. Recommend the security steering committee conduct a review.
C. Update the risk assessment at regular intervals
D. Send regular notifications directly to senior managers
Answer: (SHOW ANSWER)
Explanation
Including the impact of the risk as part of regular metrics is the best way for the information security manager to help senior management understand the related risk of having many user workstations with unpatched versions of software because it quantifies and communicates the potential consequences and likelihood of such a risk in terms of business objectives and performance indicators. Recommending the security steering committee conduct a review is not a good way because it does not provide any specific information or analysis about the risk or its impact. Updating the risk assessment at regular intervals is not a good way because it does not ensure that senior management is aware or informed about the risk or its impact. Sending regular notifications directly to senior managers is not a good way because it may be perceived as intrusive or annoying, and may not convey the severity or urgency of the risk or its impact. References:
https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-securit
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/how-to-measure-the-effectiveness-of-your-i

NEW QUESTION: 103
Of the following, whose input is of GREATEST importance in the development of an information security strategy?

A. Process owners
B. End users
C. Security architects.
D. Corporate auditors
Answer: (SHOW ANSWER)
Explanation
Process owners are the people who are responsible for the design, execution, and improvement of the business processes that support the organization's objectives and operations. Process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. Process owners also help to identify and assess the risks and impacts that the business processes face, and to define and implement the security controls and measures that can mitigate or reduce them. Process owners also facilitate the alignment and integration of the information security strategy with the business strategy, as well as the communication and collaboration among the various stakeholders and functions involved in the information security program. End users, security architects, and corporate auditors are all important stakeholders in the information security program, but they do not have the greatest importance in the development of an information security strategy. End users are the people who use the information systems and services that the information security program protects and enables. End users provide the input and feedback on the usability, functionality, and performance of the information systems and services, as well as the security awareness and behavior that they exhibit. Security architects are the people who design and implement the security architecture that supports the information security strategy. Security architects provide the input and feedback on the technical requirements, capabilities, and solutions that the information security strategy should leverage and optimize. Corporate auditors are the people who evaluate and verify the compliance and effectiveness of the information security program. Corporate auditors provide the input and feedback on the standards, regulations, and best practices that the information security strategy should follow and adhere to. Therefore, process owners have the greatest importance in the development of an information security strategy, as they provide the input and feedback on the business requirements, expectations, and priorities that the information security strategy should address and support. References = CISM Review Manual 2023, page 31 1; CISM Practice Quiz 2

NEW QUESTION: 104
A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server Which of the following would MOST effectively allow the hospital to avoid paying the ransom?
A. Employee training on ransomware
B. A properly tested offline backup system
C. A continual server replication process
D. A properly configured firewall
Answer: (SHOW ANSWER)
Explanation

The most effective way to avoid paying the ransom in a ransomware attack is to have a properly tested offline backup system. A ransomware attack is a type of cyberattack that encrypts the victim's data or systems and demands a payment for the decryption key. A properly tested offline backup system is a method of storing copies of the data or systems in a separate location that is not connected to the network or the internet. By having a properly tested offline backup system, the hospital can restore its critical server from the backup without paying the ransom or losing any data. The other options are not the most effective way to avoid paying the ransom in a ransomware attack, although they may be some preventive or detective measures. Employee training on ransomware is a preventive measure that can help raise awareness and reduce the likelihood of falling victim to phishing or other social engineering techniques that may deliver ransomware. However, it does not guarantee that employees will always follow best practices or that ransomware will not enter the network through other means. A continual server replication process is a method of creating copies of the server data or systems in real time or near real time. However, it may not be effective against ransomware, as the replication process may also copy the encrypted data or systems, making them unusable. A properly configured firewall is a preventive measure that can help block malicious network traffic and prevent unauthorized access to the server. However, it does not guarantee that ransomware will not bypass the firewall through other channels, such as email attachments or removable media.

NEW QUESTION: 105
An organization's main product is a customer-facing application delivered using Software as a Service (SaaS). The lead security engineer has just identified a major security vulnerability at the primary cloud provider. Within the organization, who is PRIMARILY accountable for the associated task?
A. The information security manager
B. The data owner
C. The application owner
D. The security engineer
Answer: (SHOW ANSWER)
Explanation
= The application owner is primarily accountable for the associated task because they are responsible for ensuring that the application meets the business requirements and objectives, as well as the security and compliance standards. The application owner is also the one who defines the roles and responsibilities of the application team, including the security engineer, and oversees the development, testing, deployment, and maintenance of the application. The application owner should work with the cloud provider to address the security vulnerability and mitigate the risk. The information security manager, the data owner, and the security engineer are not primarily accountable for the associated task, although they may have some roles and responsibilities in supporting the application owner. The information security manager is responsible for establishing and maintaining the information security program and aligning it with the business objectives and strategy. The data owner is responsible for defining the classification, usage, and protection requirements of the data. The security engineer is responsible for implementing and testing the security controls and features of the application. References = CISM Review Manual 2023, Chapter 1, Section 1.2.2, page 18; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 115.

NEW QUESTION: 106
Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?
A. Legal
B. Information security
C. Help desk
D. Human resources (HR)
Answer: (SHOW ANSWER)
Explanation
Information security is the most critical function when initiating the removal of system access for terminated employees, as it is responsible for ensuring that the access rights of the employees are revoked in a timely and effective manner, and that the security of the organization's data and systems is maintained. Information security should coordinate with other functions, such as HR, legal, and help desk, to implement the access removal process, but it is the primary function that has the authority and capability to disable or delete the access credentials of the terminated employees. The other options are not as critical as information security, as they may have different roles or responsibilities in the access removal process, or they may not have direct access to the systems or tools that control the access rights of the employees. References = CISM Review Manual 15th Edition, page 114: "Information security is responsible for ensuring that access rights are revoked in a timely and effective manner." SOC 2 Controls: Access Removal for Terminated or Transferred Users, snippets: "Systems access that is no longer required for terminated or transferred users is removed within one business day. For terminated employees, access to key IT systems is revoked in a timely manner. A termination checklist and ticket are completed, and access is revoked for employees as a component of the employee termination process." IT Involvement in Employee Termination, A Checklist, snippets: "Disable all network access. If your company uses a master access list of active passwords, tell the system to deny any passcodes associated with the user being terminated. If your system doesn't have a deny function, delete the user and their associated passwords. Monitor employee access." Human resources (HR) is the most critical function when initiating the removal of system access for terminated employees because it is responsible for notifying the relevant parties, such as information security, help desk, and legal, of the employee's termination status and date. HR also ensures that the employee's exit process is completed and documented, and that the employee returns any company-owned devices or assets.
HR also coordinates with the employee's manager and team to ensure a smooth transition of work and responsibilities.

NEW QUESTION: 107
Which of the following is MOST important when defining how an information security budget should be allocated?
A. Regulatory compliance standards
B. Information security strategy
C. Information security policy
D. Business impact assessment
Answer: (SHOW ANSWER)
Explanation
Information security strategy is the most important factor when defining how an information security budget should be allocated because it helps to align the security objectives and initiatives with the business goals and priorities. An information security strategy is a high-level plan that defines the vision, mission, scope, and direction of the security program, as well as the roles and responsibilities, governance structures, policies and standards, risk management approaches, and performance measurement methods. An information security strategy helps to identify and prioritize the security needs and requirements of the organization, as well as to allocate the resources and funding accordingly. An information security strategy also helps to communicate the value and benefits of security to the stakeholders and justify the security investments. Therefore, information security strategy is the correct answer.
References:
https://www.techtarget.com/searchsecurity/tip/Cybersecurity-budget-breakdown-and-best-practices
https://www.csoonline.com/article/3671108/how-2023-cybersecurity-budget-allocations-are-shaping-up.ht
https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

NEW QUESTION: 108
Which of the following is MOST important in order to obtain senior leadership support when presenting an information security strategy?
A. The strategy aligns with management's acceptable level of risk.
B. The strategy addresses ineffective information security controls.
C. The strategy aligns with industry benchmarks and standards.
D. The strategy addresses organizational maturity and the threat environment.
Answer: (SHOW ANSWER)
Explanation
The most important factor to obtain senior leadership support when presenting an information security strategy is that the strategy aligns with management's acceptable level of risk because it ensures that the strategy is consistent and compatible with the organization's risk appetite and thresholds, and reflects management's expectations and priorities for security risk management. The strategy addresses ineffective information security controls is not a very important factor because it does not indicate how the strategy will improve or enhance the security controls or performance. The strategy aligns with industry benchmarks and standards is not a very important factor because it does not indicate how the strategy will differentiate or innovate the organization's security capabilities or practices. The strategy addresses organizational maturity and the threat

environment is not a very important factor because it does not indicate how the strategy will advance or adapt the organization's security posture or resilience. References:
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-busin

NEW QUESTION: 109
Which of the following is the PRIMARY advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program?
A. It offers the organization flexible deployment options using cloud infrastructure.
B. It allows the organization to prioritize its core operations.
C. It is more secure than traditional data backup architecture.
D. It allows the use of a professional response team at a lower cost.
Answer: (SHOW ANSWER)
Explanation
The primary advantage of an organization using Disaster Recovery as a Service (DRaaS) to help manage its disaster recovery program is B. It allows the organization to prioritize its core operations. This is because DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster1. DRaaS can help the organization to prioritize its core operations by:
Reducing the need for provisioning and maintaining its own off-site disaster recovery environment, which can be costly, complex, and resource-intensive12 Enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment instead of from the disaster-affected physical servers, which can minimize the downtime, data loss, and business disruption12 Providing the organization with flexible and scalable deployment options, such as on-demand, pay-per-use, or subscription-based models, that can meet its changing business needs and budget12 Leveraging the expertise, experience, and best practices of the service provider, who can handle the disaster recovery planning, testing, and execution, and ensure compliance with the relevant standards and regulations12 DRaaS is a cloud computing service model that allows an organization to back up its data and IT infrastructure in a third-party cloud computing environment and provide all the disaster recovery orchestration, all through a SaaS solution, to regain access and functionality to IT infrastructure after a disaster. DRaaS can help the organization to prioritize its core operations by reducing the need for provisioning and maintaining its own off-site disaster recovery environment, enabling the organization to continue running its applications from the service provider's cloud or hybrid cloud environment, providing the organization with flexible and scalable deployment options, and leveraging the expertise, experience, and best practices of the service provider. (From CISM Manual or related resources)

NEW QUESTION: 110
Which of the following is MOST important to convey to employees in building a security risk-aware culture?

A. Personal information requires different security controls than sensitive information.
B. Employee access should be based on the principle of least privilege.
C. Understanding an information asset's value is critical to risk management.
D. The responsibility for security rests with all employees.
Answer: (SHOW ANSWER)
Explanation
= The most important message to convey to employees in building a security risk-aware culture is that the responsibility for security rests with all employees, not just the information security function or the management. A security risk-aware culture is a collective mindset of the people in the organization working every day to protect the enterprise and its information assets from internal and external threats. A security risk-aware culture requires the workforce to know the security risks and the processes for avoiding or mitigating them, and to make thoughtful decisions that align with security policies and standards. A security risk-aware culture also incorporates a broader corporate culture of day-to-day actions that encourage employees to report security incidents, share security best practices, and participate in security awareness and training programs. A security risk-aware culture helps to reduce the human factor that causes 90 percent of all cyberattacks, and to offset the impact of corrupted or lost data, decreased revenue, regulatory fines, and reputational damage. A security risk-aware culture turns people from assets that must be protected into assets that actively contribute to the cybersecurity and risk management posture and elevate security to being a business enabler rather than a business impediment123.
Personal information requires different security controls than sensitive information is a true statement, but it is not the most important message to convey to employees in building a security risk-aware culture. Personal information is any information that can identify or relate to a natural person, such as name, address, email, phone number, social security number, etc. Sensitive information is any information that is confidential, proprietary, or has a high value or impact to the organization, such as trade secrets, financial data, customer data, intellectual property, etc. Different types of information may have different legal, regulatory, contractual, or ethical obligations to protect them from unauthorized access, use, disclosure, modification, or destruction. Therefore, different security controls may be applied to personal and sensitive information based on their classification, such as encryption, access control, retention, disposal, etc. However, this message does not address the broader concept of security risk-aware culture, which is not limited to information classification and protection, but also encompasses the behaviors, attitudes, and values of the employees towards security.
Employee access should be based on the principle of least privilege is a good practice, but it is not the most important message to convey to employees in building a security risk-aware culture. The principle of least privilege states that users should only have the minimum level of access and permissions that are necessary to perform their job functions, and no more. This principle helps to reduce the risk of unauthorized or inappropriate actions, such as data leakage, fraud, sabotage, etc., by limiting the exposure and impact of user activities. However, this message does not capture the essence of security risk-aware culture, which is not only about access control, but also about the awareness, understanding, and commitment of the employees to security.
Understanding an information asset's value is critical to risk management is a valid point, but it is not the most important message to convey to employees in building a security risk-aware culture. Understanding an

information asset's value is essential to determine the potential impact and likelihood of a security risk, and to prioritize the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance. However, this message does not reflect the holistic nature of security risk-aware culture, which is not only about risk assessment, but also about risk communication, risk treatment, and risk monitoring. References = Building a Culture of Security - ISACA2 The Risk-Conscious, Security-Aware Culture: The Forgotten Critical Security Control - Cisco3 CISM ITEM DEVELOPMENT GUIDE - ISACA4

NEW QUESTION: 111
Which of the following is the MOST important consideration when determining which type of failover site to employ?
A. Reciprocal agreements
B. Disaster recovery test results
C. Recovery time objectives (RTOs)
D. Data retention requirements
Answer: (SHOW ANSWER)
Explanation
The most important consideration when determining which type of failover site to employ is the recovery time objectives (RTOs). A failover site is a backup site that can be used to restore the functionality and operations of an organization's primary site in the event of a disaster or disruption. There are different types of failover sites, such as hot sites, warm sites, and cold sites, that vary in terms of availability, cost, and complexity. A recovery time objective (RTO) is a metric that defines the maximum acceptable amount of time that an organization can tolerate to restore a system or an application after a disaster or disruption. By determining the RTOs for each system or application, the organization can choose the most suitable type of failover site that can meet its recovery needs and expectations. For example, if the RTO for a critical system is very low, the organization may opt for a hot site that can provide immediate failover and minimal downtime. However, if the RTO for a non-critical system is high, the organization may choose a cold site that requires manual setup and activation, but has lower cost and maintenance. The other options are not the most important consideration when determining which type of failover site to employ, although they may be some factors or constraints that affect the decision. Reciprocal agreements are arrangements between two or more organizations that agree to provide backup facilities or resources to each other in case of a disaster or disruption. Reciprocal agreements can help reduce the cost and complexity of setting up and maintaining a failover site, but they may not guarantee the availability or compatibility of the backup facilities or resources. Disaster recovery test results are outcomes of testing and validating the functionality and performance of a failover site. Disaster recovery test results can help evaluate and improve the effectiveness and efficiency of a failover site, but they do not determine which type of failover site to employ. Data retention requirements are policies and regulations that define how long and in what format an organization must store its data. Data retention requirements can affect the design and configuration of a failover site, but they do not dictate which type of failover site to employ

NEW QUESTION: 112
A cloud application used by an organization is found to have a serious vulnerability. After assessing the risk, which of the following would be the information security manager's BEST course of action?

A. Instruct the vendor to conduct penetration testing.
B. Suspend the connection to the application in the firewall
C. Report the situation to the business owner of the application.
D. Initiate the organization's incident response process.
Answer: (SHOW ANSWER)
Explanation
= Initiating the organization's incident response process is the best course of action for the information security manager when a cloud application used by the organization is found to have a serious vulnerability.
The incident response process is a set of predefined steps and procedures that aim to contain, analyze, resolve, and learn from security incidents. The information security manager should follow the incident response process to ensure that the vulnerability is properly reported, assessed, mitigated, and communicated to the relevant stakeholders. The incident response process should also involve the cloud service provider (CSP) and the business owner of the application, as they are responsible for the security and functionality of the cloud application. Instructing the vendor to conduct penetration testing, suspending the connection to the application in the firewall, and reporting the situation to the business owner of the application are all possible actions that may be taken as part of the incident response process, but they are not the best initial course of action.
Penetration testing may help to identify the root cause and the impact of the vulnerability, but it may also cause further damage or disruption to the cloud application. Suspending the connection to the application in the firewall may prevent unauthorized access or exploitation of the vulnerability, but it may also affect the availability and continuity of the cloud application. Reporting the situation to the business owner of the application is an important step to inform them of the risk and the potential business impact, but it is not sufficient to address the vulnerability and its consequences. Therefore, the information security manager should initiate the incident response process as the best course of action, and then perform the other actions as appropriate based on the incident response plan and the risk assessment. References = CISM Review Manual
2023, page 211 1; CISM Practice Quiz 2

NEW QUESTION: 113
An organization's information security team presented the risk register at a recent information security steering committee meeting. Which of the following should be of MOST concern to the committee?
A. No owners were identified for some risks.
B. Business applications had the highest number of risks.
C. Risk mitigation action plans had no timelines.
D. Risk mitigation action plan milestones were delayed.
Answer: (SHOW ANSWER)
Explanation
The most concerning issue for the information security steering committee should be that no owners were identified for some risks in the risk register. This means that there is no clear accountability and responsibility for managing and mitigating those risks, and that the risks may not be properly addressed or monitored. The risk owners are the persons who have the authority and ability to implement the risk treatment options and to

accept the residual risk. The risk owners should be identified and assigned for each risk in the risk register, and they should report the status and progress of the risk management activities to the information security steering committee.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Management, Subsection: Risk Register, Page 104.

NEW QUESTION: 114
When developing a business case to justify an information security investment, which of the following would BEST enable an informed decision by senior management?
A. The information security strategy
B. Losses due to security incidents
C. The results of a risk assessment
D. Security investment trends in the industry
Answer: C (LEAVE A REPLY)
Explanation
The results of a risk assessment would best enable an informed decision by senior management when developing a business case to justify an information security investment. A risk assessment will help to identify and prioritize the threats and vulnerabilities that affect the organization's assets and processes, as well as the potential impact and likelihood of occurrence. A risk assessment will also provide a basis for selecting and evaluating the effectiveness of controls to mitigate the risks. According to CISA, developing a business case for security will be based on an in-depth understanding of organizational vulnerabilities, operational priorities, and return on investment1. The information security strategy, losses due to security incidents, and security investment trends in the industry are possible inputs or outputs of a risk assessment, but they are not sufficient to enable an informed decision by senior management. References: 1: The Business Case for Security - CISA 2: The Business Case for Security | CISA 3: #HowTo: Build a Business Case for Cybersecurity Investment 4: Making the Business Case for Information Security

NEW QUESTION: 115
When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:
A. best practices.
B. control framework
C. regulatory requirements.
D. cost-benefit analysis,
Answer: (SHOW ANSWER)
Explanation
Cost-benefit analysis (CBA) is a method of comparing the costs and benefits of different alternatives for achieving a desired outcome. CBA can help information security managers to choose the best controls to mitigate risk to acceptable levels by providing a rational and objective basis for decision making. CBA can also help information security managers to justify their choices to senior management, stakeholders, and auditors

by demonstrating the value and return on investment of the selected controls. CBA can also help information security managers to prioritize and allocate resources for implementing and maintaining the controls12.
CBA involves the following steps12:
Identify the objectives and scope of the analysis
Identify the alternatives and options for achieving the objectives
Identify and quantify the costs and benefits of each alternative
Compare the costs and benefits of each alternative using a common metric or criteria Select the alternative that maximizes the net benefit or minimizes the net cost Perform a sensitivity analysis to test the robustness and validity of the results Document and communicate the results and recommendations CBA is mainly driven by the information security manager's decision, but it can also take into account other factors such as best practices, control frameworks, and regulatory requirements. However, these factors are not the primary drivers of CBA, as they may not always reflect the specific needs and context of the organization.
Best practices are general guidelines or recommendations that may not suit every situation or environment. Control frameworks are standardized models or methodologies that may not cover all aspects or dimensions of information security. Regulatory requirements are mandatory rules or obligations that may not address all risks or threats faced by the organization. Therefore, CBA is the best method to choose the most appropriate and effective controls to mitigate risk to acceptable levels, as it considers the costs and benefits of each control in relation to the organization's objectives, resources, and environment12. References = CISM Domain 2: Information Risk Management (IRM) [2022 update], Five Key Considerations When Developing Information Security Risk Treatment Plans

NEW QUESTION: 116
Which of the following is MOST important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals?
A. Skills required for the incident response team
B. A list of external resources to assist with incidents
C. Service level agreements (SLAs)
D. A detailed incident notification process
Answer: (SHOW ANSWER)
Explanation
A detailed incident notification process is most important to include in an incident response plan to ensure incidents are responded to by the appropriate individuals. The incident notification process defines the roles and responsibilities of the incident response team members, the escalation procedures, the communication channels, the reporting requirements, and the stakeholders to be informed. The incident notification process helps to ensure that the right people are involved in the incident response, that the incident is handled in a timely and efficient manner, and that the relevant information is shared with the appropriate parties. Skills required for the incident response team, a list of external resources to assist with incidents, and service level agreements (SLAs) are also important elements of an incident response plan, but they are not as critical as the incident notification process. Skills required for the incident response team describe the competencies and qualifications of the team members, but they do not specify who should be notified or involved in the incident response. A list of external resources to assist with incidents provides a directory of external parties that can

provide support or expertise in the incident response, but it does not define the criteria or process for engaging them. Service level agreements (SLAs) define the expectations and obligations of the service providers and the service recipients in the incident response, but they do not detail the steps or procedures for notifying or escalating incidents. References = CISM Review Manual, 16th Edition, pages 191-1921; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 662

NEW QUESTION: 117
Company A, a cloud service provider, is in the process of acquiring Company B to gain new benefits by incorporating their technologies within its cloud services.
Which of the following should be the PRIMARY focus of Company A's information security manager?
A. The organizational structure of Company B
B. The cost to align to Company A's security policies
C. Company A's security architecture
D. Company B's security policies
Answer: (SHOW ANSWER)
Explanation
According to the CISM Review Manual, the security architecture of an organization defines the security principles, standards, guidelines and procedures that support the information security strategy and align with the business objectives. When acquiring another company, the information security manager of the acquiring company should focus on ensuring that the security architecture of the acquired company is compatible with its own, or that any gaps or conflicts are identified and resolved.
References = CISM Review Manual, 27th Edition, Chapter 2, Section 2.1.2, page 751.

NEW QUESTION: 118
A new regulatory requirement affecting an organization's information security program is released. Which of the following should be the information security manager's FIRST course of action?
A. Perform a gap analysis.
B. Conduct benchmarking.
C. Notify the legal department.
D. Determine the disruption to the business.
Answer: (SHOW ANSWER)
Explanation
= A new regulatory requirement affecting an organization's information security program is released. The information security manager's first course of action should be to notify the legal department, as they are responsible for ensuring compliance with the relevant laws and regulations. The legal department can advise the information security manager on how to interpret and implement the new requirement, as well as what are the potential implications and risks for the organization12.
References = 1: CISM Review Manual (Digital Version), page 271 2: CISM Review Manual (Print Version), page 271 Learn more:
1. isaca.org2. csoonline.com

NEW QUESTION: 119
Which of the following BEST enables an organization to transform its culture to support information security?
A. Periodic compliance audits
B. Strong management support
C. Robust technical security controls
D. Incentives for security incident reporting
Answer: (SHOW ANSWER)
Explanation
According to the CISM Review Manual (Digital Version), page 5, information security culture is the set of values, attitudes, and behaviors that shape how an organization and its employees view and practice information security. Transforming the information security culture requires a change management process that involves the following steps: creating a sense of urgency, forming a powerful coalition, developing a vision and strategy, communicating the vision, empowering broad-based action, generating short-term wins, consolidating gains and producing more change, and anchoring new approaches in the culture1. Among the four options, strong management support is the best enabler for transforming the information security culture, as it can provide the necessary leadership, resources, sponsorship, and alignment for the change management process. Periodic compliance audits, robust technical security controls, and incentives for security incident reporting are important elements of information security, but they are not sufficient to change the culture without strong management support. References = 1: CISM Review Manual (Digital Version), page 5

NEW QUESTION: 120
During which of the following development phases is it MOST challenging to implement security controls?

A. Post-implementation phase
B. Implementation phase
C. Development phase
D. Design phase
Answer: (SHOW ANSWER)
Explanation
The development phase is the stage of the system development life cycle (SDLC) where the system requirements, design, architecture, and implementation are performed. The development phase is most challenging to implement security controls because it involves complex and dynamic processes that may not be well understood or documented. Security controls are essential for ensuring the confidentiality, integrity, and availability of the system and its data, as well as for complying with regulatory and contractual obligations. However, security controls may also introduce additional costs, risks, and constraints to the development process, such as:
Increased complexity and overhead of testing, verification, validation, and maintenance Reduced flexibility and agility of changing requirements or design Increased dependency on external vendors or third parties for security services or products Increased vulnerability to errors, defects, or vulnerabilities in the code or configuration Increased difficulty in measuring and reporting on security performance or effectiveness

Therefore, implementing security controls in the development phase requires careful planning, coordination, communication, and collaboration among all stakeholders involved in the SDLC. It also requires a clear understanding of the security objectives, scope, criteria, standards, policies, procedures, roles, responsibilities, and resources for the system. Moreover, it requires a proactive approach to identifying and mitigating potential threats or risks that may affect the security of the system.
References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1: System Development Life Cycle (SDLC)2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 121
Penetration testing is MOST appropriate when a:
A. new system is about to go live.
B. new system is being designed.
C. security policy is being developed.
D. security incident has occurred,
Answer: (SHOW ANSWER)
Explanation
= Penetration testing is most appropriate when a new system is about to go live, because it is a method of evaluating the security of a system by simulating an attack from a malicious source. Penetration testing can help to identify and exploit vulnerabilities, assess the impact and risk of a breach, and provide recommendations for remediation and improvement. Penetration testing can also help to validate the effectiveness of the security controls and policies implemented for the new system, and ensure compliance with relevant standards and regulations. Penetration testing is usually performed after the system has undergone other types of testing, such as functional, performance, and usability testing, and before the system is deployed to the production environment. Penetration testing is not as appropriate when a new system is being designed, because the system is still in the early stages of development and may not have all the features and functionalities implemented. Penetration testing at this stage may not provide a realistic or comprehensive assessment of the system's security, and may cause delays or disruptions in the development process.
Penetration testing is also not as appropriate when a security policy is being developed, because the policy is a high-level document that defines the goals, objectives, and principles of information security for the organization. Penetration testing is a technical and operational activity that tests the implementation and enforcement of the policy, not the policy itself. Penetration testing is also not as appropriate when a security incident has occurred, because the incident may have already compromised the system and caused damage or loss. Penetration testing at this stage may not be able to prevent or mitigate the incident, and may interfere with the incident response and recovery efforts. Penetration testing after an incident may be useful for forensic analysis and lessons learned, but it is not the primary or immediate response to an incident. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 229-230, 233-234.

NEW QUESTION: 122
An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification for granting an exception to the policy?
A. The benefit is greater than the potential risk.
B. USB storage devices are enabled based on user roles.
C. Users accept the risk of noncompliance.
D. Access is restricted to read-only.
Answer: (SHOW ANSWER)
Explanation
The strongest justification for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. A security policy is a document that defines the goals, objec-tives, principles, roles, responsibilities, and requirements for protecting information and systems in an organization. A security policy should be based on a risk assessment that identifies and evaluates the threats and vulnerabilities that affect the organiza-tion's assets, as well as the potential impact and likelihood of incidents. A security pol-icy should also be aligned with the organization's business objectives and risk appe-tite1. However, there may be situations where a security policy cannot be fully enforced or complied with due to technical, operational, or business reasons. In such cases, an exception to the policy may be requested and granted by an authorized person or body, such as a security manager or a policy committee. An exception to a security policy should be justified by a clear and compelling reason that outweighs the risk of non-compliance. An exception to a security policy should also be documented, approved, monitored, reviewed, and revoked as necessary2. The strongest justification for grant-ing an exception to the security policy that disables access to USB storage devices on laptops and desktops is that the benefit is greater than the potential risk. USB storage devices are portable devices that can store large amounts of data and can be easily connected to laptops and desktops via USB ports. They can provide several benefits for users and organizations, such as:
*Enhancing data mobility and accessibility
*Improving data backup and recovery
*Supporting data sharing and collaboration
*Enabling data encryption and authentication
However, USB storage devices also pose significant security risks for users and organi-zations, such as:
*Introducing malware or viruses to laptops and desktops
*Exposing sensitive data to unauthorized access or disclosure
*Losing or stealing data due to device loss or theft
*Violating security policies or regulations

Therefore, an exception to the security policy that disables access to USB storage de-vices on laptops and desktops should only be granted if the benefit of using them is greater than the potential risk of compromising them. For example, if a user needs to transfer a large amount of data from one laptop to another in a remote location where there is no network connection available, and the data is encrypted and protected by a strong password on the USB device, then the benefit of using the USB device may be greater than the risk of losing or exposing it. The other options are not the strongest justifications for granting an exception to the security policy that disables access to USB storage devices on laptops and desktops. Enabling USB storage devices based on user roles is not a justification, but rather a possible way of implementing a more gran-ular or flexible security policy that allows different levels of access for different types of users3. Users accepting the risk of noncompliance is not a justification, but rather a requirement for requesting an exception to a security policy that acknowledges their responsibility and accountability for any consequences of noncompliance4. Accessing being restricted to read-only is not a justification, but rather a possible control that can reduce the risk of introducing malware or viruses from USB devices to laptops and desktops5. References: 1: Information Security Policy - NIST 2: Policy Exception Man-agement - ISACA 3: Deploy and manage Removable Storage Access Control using In-tune - Microsoft Learn 4: Policy Exception Request Form - University of California 5: Re-movable Media Policy Writing Tips - CurrentWare

NEW QUESTION: 123
Which of the following should be the MOST important consideration of business continuity management?
A. Ensuring human safety
B. Identifying critical business processes
C. Ensuring the reliability of backup data
D. Securing critical information assets
Answer: (SHOW ANSWER)
Explanation
= Business continuity management (BCM) is the process of planning and implementing measures to ensure the continuity of critical business processes in the event of a disruption. The most important consideration of BCM is ensuring human safety, as this is the primary responsibility of any organization and the basis of ethical conduct. Human safety includes protecting the health and well-being of employees, customers, suppliers, and other stakeholders who may be affected by a disruption. Identifying critical business processes, ensuring the reliability of backup data, and securing critical information assets are also important aspects of BCM, but they are secondary to human safety. References = CISM Review Manual, 16th Edition, ISACA, 2020, p. 2111; CISM Online Review Course, Domain 4: Information Security Incident Management, Module 4: Business Continuity and Disaster Recovery, ISACA2

NEW QUESTION: 124
Which of the following is the MOST important requirement for a successful security program?
A. Mapping security processes to baseline security standards
B. Penetration testing on key systems
C. Management decision on asset value
D. Nondisclosure agreements (NDA) with employees

Answer: (SHOW ANSWER)

Explanation

"A successful security program requires management support and involvement. One of the key aspects of management support is to decide on the value of assets and the acceptable level of risk for them. This will help define the security objectives and priorities for the program. The other options are possible activities within a security program, but they are not as important as management decision on asset value."

NEW QUESTION: 125

The effectiveness of an information security governance framework will BEST be enhanced if:

A. consultants review the information security governance framework.

B. a culture of legal and regulatory compliance is promoted by management.

C. risk management is built into operational and strategic activities.

D. IS auditors are empowered to evaluate governance activities

Answer: (SHOW ANSWER)

Explanation

The effectiveness of an information security governance framework will best be enhanced if risk management is built into operational and strategic activities. This is because risk management is a key component of information security governance, which is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are effectively managed and measured. Risk management involves identifying, analyzing, evaluating, treating, monitoring, and communicating information security risks that may affect the organization's objectives, assets, and stakeholders. By integrating risk management into operational and strategic activities, the organization can ensure that information security risks are considered and addressed in every decision and action, and that the information security governance framework is aligned with the organization's risk appetite and tolerance. This also helps to optimize the allocation of resources, enhance the performance and value of information security, and improve the accountability and transparency of information security governance.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Governance Framework, page 181; CISM Review Manual, 16th Edition, Chapter 2: Information Risk Management, Section: Risk Management, page 812; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 53, page 493.

NEW QUESTION: 126

Of the following, who is accountable for data loss in the event of an information security incident at a third-party provider?

A. The information security manager

B. The service provider that hosts the data

C. The incident response team

D. The business data owner

Answer: (SHOW ANSWER)

Explanation

The business data owner is accountable for data loss in the event of an information security incident at a third-party provider because they are ultimately responsible for the protection and use of their data, regardless of where it is stored or processed. The information security manager is not accountable for data loss at a third-party provider, but rather responsible for implementing and enforcing the security policies and standards that govern the relationship with the provider. The service provider that hosts the data is not accountable for data loss at their site, but rather liable for any breach of contract or service level agreement that may result from such an incident. The incident response team is not accountable for data loss at a third-party provider, but rather responsible for responding to and managing the incident according to the incident response plan.
References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cl
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 127
Which of the following is the BEST justification for making a revision to a password policy?
A. Vendor recommendation
B. Audit recommendation
C. A risk assessment
D. Industry best practice
Answer: (SHOW ANSWER)
Explanation
The best justification for making a revision to a password policy is a risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of information assets and systems. By conducting a risk assessment, the organization can determine the appropriate level of security controls and measures to protect its information assets and systems, including password policies. A risk assessment can also help identify any gaps or weaknesses in the existing password policy, and provide recommendations for improvement based on the organization's risk appetite and tolerance. The other options are not the best justification for making a revision to a password policy, although they may be some inputs or outputs of the risk assessment process. A vendor recommendation is an external source of advice or guidance that may or may not be relevant or applicable to the organization's specific context and needs. A vendor recommendation should not be followed blindly without conducting a risk assessment to evaluate its suitability and effectiveness. An audit recommendation is an internal source of feedback or suggestion that may or may not be accurate or complete. An audit recommendation should not be implemented without conducting a risk assessment to verify its validity and feasibility. An industry best practice is a general standard or guideline that may or may not reflect the organization's unique characteristics and requirements. An industry best practice should not be adopted without conducting a risk assessment to customize it according to the organization's goals and priorities

NEW QUESTION: 128
A recovery point objective (RPO) is required in which of the following?
A. Disaster recovery plan (DRP)

B. Information security plan
C. Incident response plan
D. Business continuity plan (BCP)
Answer: (SHOW ANSWER)
Explanation
A recovery point objective (RPO) is required in a disaster recovery plan (DRP), because it indicates the earliest point in time to which it is acceptable to recover data after a disaster. It effectively quantifies the permissible amount of data loss in case of interruption. It is determined based on the acceptable data loss in case of disruption of operations1. A DRP is a document that defines the procedures, resources, and actions to restore the critical IT systems and data in the event of a disaster that affects the normal operations of the organization2. A DRP should include the RPO for each critical system and data, as well as the backup and restoration methods, frequency, and location to achieve the RPO3.
A RPO is not required in an information security plan, an incident response plan, or a business continuity plan (BCP), because these plans have different purposes and scopes. An information security plan is a document that defines the objectives, policies, standards, and guidelines for information security management in the organization4. An incident response plan is a document that defines the procedures, roles, and responsibilities for identifying, analyzing, responding to, and learning from security incidents that may compromise the confidentiality, integrity, or availability of information assets. A BCP is a document that defines the procedures, resources, and actions to ensure the continuity of the essential business functions and processes in the event of a disruption that affects the normal operations of the organization. These plans may include other metrics, such as recovery time objective (RTO), which is the amount of time after a disaster in which business operation is resumed, or resources are again available for use, but they do not require a RPO.
References = 1: IS Disaster Recovery Objectives - RunModule 2: Information System Contingency Planning Guidance - ISACA 3: CISM Certified Information Security Manager - Question1411 4: CISM Review Manual, 16th Edition, ISACA, 2021, page 23. : CISM Review Manual, 16th Edition, ISACA, 2021, page 223.: CISM Review Manual, 16th Edition, ISACA, 2021, page 199. : RTO vs. RPO - What is the difference? - Advisera

NEW QUESTION: 129
Which of the following is MOST important to complete during the recovery phase of an incident response process before bringing affected systems back online?
A. Document recovery steps for senior management reporting.
B. Test and verify that compromisedsystems are clean.
C. Capture and preserve forensic images of affected systems.
D. Record and close security incident tickets.
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following is the MOST appropriate metric to demonstrate the effectiveness of information security controls to senior management?

A. Downtime due to malware infections
B. Number of security vulnerabilities uncovered with network scans

C. Percentage of servers patched
D. Annualized loss resulting from security incidents
Answer: D (LEAVE A REPLY)
Explanation
Annualized loss resulting from security incidents is the most appropriate metric to demonstrate the effectiveness of information security controls to senior management, as it quantifies the financial impact of security breaches on the organization's assets, operations, and reputation. This metric helps to communicate the value of security investments, justify the security budget, and prioritize the security initiatives based on the potential loss reduction. Annualized loss resulting from security incidents can be calculated by multiplying the annualized rate of occurrence (ARO) of an incident by the single loss expectancy (SLE) of an incident. ARO is the estimated frequency of an incident occurring in a year, and SLE is the estimated cost of an incident. For example, if an organization estimates that a ransomware attack may occur once every two years, and that each attack may cost $100,000 to recover, then the annualized loss resulting from ransomware attacks is $50,000 ($100,000 / 2).
References = CISM Review Manual 2022, page 3171; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.112; Key Performance Indicators for Security Governance, Part 1; Performance Measurement Guide for Information Security

NEW QUESTION: 131
An incident response team has been assembled from a group of experienced individuals, Which type of exercise would be MOST beneficial for the team at the first drill?
A. Red team exercise
B. Black box penetration test
C. Disaster recovery exercise
D. Tabletop exercise
Answer: (SHOW ANSWER)
Explanation
= A tabletop exercise is the best type of exercise for an incident response team at the first drill, as it is a low-cost, low-risk, and high-value method to test and evaluate the incident response plan, procedures, roles, and capabilities. A tabletop exercise is a simulation of a realistic scenario that involves a security incident, and requires the participation and discussion of the incident response team members and other relevant stakeholders. The tabletop exercise allows the incident response team to identify and address the gaps, issues, or challenges in the incident response process, and to improve the communication, coordination, and collaboration among the team members and other parties. The tabletop exercise also helps to enhance the knowledge, skills, and confidence of the incident response team members, and to prepare them for more complex or advanced exercises or real incidents.
A red team exercise (A) is a type of exercise that involves a group of ethical hackers or security experts who act as adversaries and attempt to compromise the organization's security defenses, systems, or processes. A red team exercise is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a red team exercise is not the best type of exercise for an incident response team at the first drill, as

it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
A black box penetration test (B) is a type of security testing that simulates a malicious attack on the organization's systems or processes, without any prior knowledge or information about them. A black box penetration test is a high-cost, high-risk, and high-value method to test and evaluate the security posture and resilience of the organization, and to identify and exploit the security weaknesses or vulnerabilities. However, a black box penetration test is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
A disaster recovery exercise is a type of exercise that simulates a catastrophic event that disrupts or destroys the organization's critical systems or processes, and requires the activation and execution of the disaster recovery plan, procedures, roles, and capabilities. A disaster recovery exercise is a high-cost, high-risk, and high-value method to test and evaluate the disaster recovery posture and resilience of the organization, and to identify and address the recovery issues or challenges. However, a disaster recovery exercise is not the best type of exercise for an incident response team at the first drill, as it is more suitable for a mature and experienced team that has already tested and validated the incident response plan, procedures, roles, and capabilities.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, Subsection: Testing and Maintenance, page 184-1851

NEW QUESTION: 132
Which of the following is the BEST way to ensure the organization's security objectives are embedded in business operations?
A. Publish adopted information security standards.
B. Perform annual information security compliance reviews.
C. Implement an information security governance framework.
D. Define penalties for information security noncompliance.
Answer: (SHOW ANSWER)
Explanation
The best way to ensure the organization's security objectives are embedded in business operations is to implement an information security governance framework. An information security governance framework is a set of policies, procedures, standards, guidelines, roles, and responsibilities that define and direct how the organization manages and measures its information security activities. An information security governance framework helps to align the information security strategy with the business strategy and the organizational culture, and to ensure that the information security objectives are consistent with the business objectives and the stakeholder expectations. An information security governance framework also helps to establish the authority, accountability, and communication channels for the information security function, and to provide the necessary resources, tools, and controls to implement and monitor the information security program. By implementing an information security governance framework, the organization can embed the information security objectives in business operations, and ensure that the information security function supports and enables the business processes and functions, rather than hinders or restricts them.

References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Governance Framework, page 181; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 75, page 702.

NEW QUESTION: 133
Which of the following is BEST to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate?
A. Projected Increase in maturity level
B. Estimated reduction in risk
C. Projected costs over time
D. Estimated increase in efficiency
Answer: B (LEAVE A REPLY)
Explanation
The best thing to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate is an estimated reduction in risk. Risk reduction is the expected benefit of implementing an information security initiative, as it reduces the likelihood and impact of threats and vulnerabilities that may affect the organization's information assets and systems. By estimating the reduction in risk, the information security manager can demonstrate the value and benefits of the information security initiative to the organization's performance, reputation, and competitiveness. The information security manager can also compare the estimated reduction in risk with the estimated cost of the information security initiative to determine its cost-effectiveness and feasibility. The other options are not the best thing to include in a business case, although they may be some inputs or outputs of the risk assessment process. A projected increase in maturity level is a potential outcome of implementing an information security initiative, as it improves the organization's capabilities and processes for managing information security risks. However, it does not necessarily reflect the actual reduction in risk or the ROI of the information security initiative. A projected cost over time is a component of calculating the ROI of an information security initiative, as it reflects the total cost of ownership and maintenance of the initiative. However, it does not indicate the expected benefit or value of the initiative. An estimated increase in efficiency is a possible benefit of implementing an information security initiative, as it may enhance the organization's productivity and performance. However, it may not be directly related to the reduction in risk or the ROI of the information security initiative.

NEW QUESTION: 134
The MOST important element in achieving executive commitment to an information security governance program is:
A. a defined security framework.
B. a process improvement model
C. established security strategies.
D. identified business drivers.
Answer: D (LEAVE A REPLY)
Explanation

The most important element in achieving executive commitment to an information security governance program is to align the program with the identified business drivers of the organization. Business drivers are the factors that influence the strategic objectives, goals, and priorities of the organization. They reflect the needs and expectations of the stakeholders, customers, regulators, and other parties that are relevant to the organization's mission and vision. By aligning the information security governance program with the business drivers, the executive can demonstrate the value and benefits of information security to the organization's performance, reputation, and competitiveness. The other options are not the most important element, although they may be part of an information security governance program. A defined security framework is a set of standards, guidelines, and best practices that provide a structure and direction for implementing information security. A process improvement model is a methodology that helps to identify, analyze, and improve the processes related to information security. Established security strategies are the plans and actions that define how information security supports and enables the business objectives and goals. These elements are important for developing and executing an information security governance program, but they do not necessarily ensure executive commitment unless they are aligned with the business drivers

NEW QUESTION: 135
Which of the following is the BEST way to ensure the business continuity plan (BCP) is current?
A. Manage business process changes.
B. Update business impact analyses (BIAs) on a regular basis.
C. Conduct periodic testing.
D. Review and update emergency contact lists.
Answer: (SHOW ANSWER)
Explanation
Conducting periodic testing is the best way to ensure the BCP is current because it can validate the effectiveness and efficiency of the BCP, identify any gaps or weaknesses, and provide feedback and recommendations for improvement. Testing can also verify that the BCP reflects the current business environment, processes, and requirements, and that the BCP team members are familiar with their roles and responsibilities.
References: The CISM Review Manual 2023 states that "testing is a critical component of the BCP process" and that "testing can help ensure that the BCP is current, effective, and efficient, and that it meets the business objectives and expectations" (p. 195). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Conducting periodic testing is the correct answer because it is the best way to ensure the BCP is current, as it can evaluate the BCP against the current business environment, processes, and requirements, and identify any areas for improvement or update" (p. 98).
Additionally, the article Business Continuity Planning: Testing an Organization's Plan from the ISACA Journal 2019 states that "testing is essential to ensure that the BCP is current and effective" and that "testing can provide assurance that the BCP is aligned with the business needs and expectations, and that the BCP team members are competent and confident in executing their tasks" (p. 1)

NEW QUESTION: 136

To ensure that a new application complies with information security policy, the BEST approach is to:
A. review the security of the application before implementation.
B. integrate functionality the development stage.
C. perform a vulnerability analysis.
D. periodically audit the security of the application.
Answer: (SHOW ANSWER)
Explanation
Performing a vulnerability analysis is the best option to ensure that a new application complies with information security policy because it helps to identify and evaluate any security flaws or weaknesses in the application that may expose it to potential threats or attacks, and provide recommendations or solutions to mitigate them. Reviewing the security of the application before implementation is not a good option because it may not detect or prevent all security issues that may arise after implementation or deployment. Integrating security functionality at the development stage is not a good option because it may not account for all security requirements or challenges of the application or its environment. Periodically auditing the security of the application is not a good option because it may not address any security issues that may occur between audits or after deployment. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software-development-lifecycle
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

NEW QUESTION: 137
Which of the following BEST enables an organization to maintain an appropriate security control environment?
A. Alignment to an industry security framework
B. Budgetary support for security
C. Periodic employee security training
D. Monitoring of the threat landscape
Answer: A (LEAVE A REPLY)
Explanation
Alignment to an industry security framework ensures that the organization adopts best practices and standards for security control implementation and maintenance. References = CISM Review Manual, 16th Edition, Domain 1: Information Security Governance, Chapter 1: Establish and Maintain an Information Security Strategy, Section: Information Security Frameworks

NEW QUESTION: 138

Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?
A. Updated security policies
B. Defined security standards
C. Threat intelligence
D. Regular antivirus updates
Answer: C (LEAVE A REPLY)
Explanation
Threat intelligence is the most helpful method for protecting an enterprise from advanced persistent threats (APTs), as it provides relevant and actionable information about the sources, methods, and intentions of the adversaries who conduct APTs. Threat intelligence can help to identify and anticipate the APTs that target the enterprise, as well as to enhance the detection, prevention, and response capabilities of the information security program. Threat intelligence can also help to reduce the impact and duration of the APTs, as well as to improve the resilience and recovery of the enterprise. Threat intelligence can be obtained from various sources, such as internal data, external feeds, industry peers, government agencies, or security vendors.
The other options are not as helpful as threat intelligence, as they do not provide a specific and timely way to protect the enterprise from APTs. Updated security policies are important to establish the rules, roles, and responsibilities for information security within the enterprise, as well as to align the information security program with the business objectives, standards, and regulations. However, updated security policies alone are not enough to protect the enterprise from APTs, as they do not address the dynamic and sophisticated nature of the APTs, nor do they provide the technical or operational measures to counter the APTs. Defined security standards are important to specify the minimum requirements and best practices for information security within the enterprise, as well as to ensure the consistency, quality, and compliance of the information security program. However, defined security standards alone are not enough to protect the enterprise from APTs, as they do not account for the customized and targeted nature of the APTs, nor do they provide the situational or contextual awareness to deal with the APTs. Regular antivirus updates are important to keep the antivirus software up to date with the latest signatures and definitions of the known malware, viruses, and other malicious code. However, regular antivirus updates alone are not enough to protect the enterprise from APTs, as they do not detect or prevent the unknown or zero-day malware, viruses, or other malicious code that are often used by the APTs, nor do they provide the behavioral or heuristic analysis to identify the APTs.
References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 211-212, 215-216, 233-234, 237-238.
CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1021.
Advanced Persistent Threats and Nation-State Actors 1
Book Review: Advanced Persistent Threats 2
Advanced Persistent Threat (APT) Protection 3
Establishing Advanced Persistent Security to Combat Long-Term Threats 4 What is the difference between Anti - APT (Advanced Persistent Threat) and ATP (Advanced Threat Protection)5

NEW QUESTION: 139
The PRIMARY advantage of involving end users in continuity planning is that they:
A. have a better understanding of specific business needs.
B. are more objective than information security management.

C. can see the overall impact to the business.
D. can balance the technical and business risks.
Answer: (SHOW ANSWER)
Explanation
= End users are the primary stakeholders of the business processes and functions that need to be protected and recovered in the event of a disruption. They have the most knowledge and experience of the specific business needs, requirements, and dependencies that affect the continuity planning. Involving them in the planning process can help to ensure that the continuity plan is aligned with the business objectives and expectations, and that the critical activities and resources are prioritized and protected accordingly. End users can also provide valuable feedback and suggestions to improve the plan and its implementation. References = CISM Review Manual 15th Edition, page 2291; CISM Practice Quiz, question 1182

NEW QUESTION: 140
Which of the following should an information security manager do FIRST when a mandatory security standard hinders the achievement of an identified business objective?

A. Revisit the business objective.
B. Escalate to senior management.
C. Perform a cost-benefit analysis.
D. Recommend risk acceptance.
Answer: (SHOW ANSWER)
Explanation
Escalate to senior management, because this could help the information security manager to inform the decision-makers of the situation, explain the implications and trade-offs, and seek their guidance and approval for the next steps2. However, this answer is not certain, and you might need to consider other factors as well.

NEW QUESTION: 141
When establishing an information security governance framework, it is MOST important for an information security manager to understand:
A. risk management techniques.
B. information security best practices.
C. the threat environment.
D. the corporate culture.
Answer: (SHOW ANSWER)

NEW QUESTION: 142
Which of the following is the BEST course of action for an information security manager to align security and business goals?
A. Conducting a business impact analysis (BIA)
B. Reviewing the business strategy
C. Defining key performance indicators (KPIs)
D. Actively engaging with stakeholders

Answer: (SHOW ANSWER)

Explanation

= According to the CISM Review Manual, the information security manager should actively engage with stakeholders to align security and business goals. This means understanding the business needs, expectations, and risk appetite of the stakeholders, and communicating the value and benefits of security initiatives to them.

By engaging with stakeholders, the information security manager can also gain their support and commitment for security programs and projects, and ensure that security objectives are aligned with business strategy and priorities. References = CISM Review Manual, 16th Edition, ISACA, 2020, page 23.

NEW QUESTION: 143

Relationships between critical systems are BEST understood by

A. evaluating key performance indicators (KPIs)

B. performing a business impact analysis (BIA)

C. developing a system classification scheme

D. evaluating the recovery time objectives (RTOs)

Answer: (SHOW ANSWER)

Explanation

The explanation given is: "A BIA is a process that identifies and evaluates the potential effects of natural and man-made events on business operations. It helps to understand how critical systems are interrelated and what their dependencies are. A BIA also helps to determine the RTOs for each system. The other options are not directly related to understanding the relationships between critical systems."

NEW QUESTION: 144

To help ensure that an information security training program is MOST effective its contents should be

A. focused on information security policy.

B. aligned to business processes

C. based on employees' roles

D. based on recent incidents

Answer: (SHOW ANSWER)

Explanation

"An information security training program should be tailored to the specific roles and responsibilities of employees. This will help them understand how their actions affect information security and what they need to do to protect it. A generic training program that is focused on policy, business processes or recent incidents may not be relevant or effective for all employees."

NEW QUESTION: 145

An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?

A. Initiate incident response.

B. Disable remote

C. Initiate a device reset.
D. Conduct a risk assessment.
Answer: (SHOW ANSWER)
Explanation
Initiating incident response is the first course of action for an information security manager when an employee reports the loss of a personal mobile device containing corporate information. This will help to contain the incident, assess the impact, and take appropriate measures to prevent or mitigate further damage. According to ISACA, incident management is one of the key processes for information security governance. Initiating a device reset, disabling remote access, and conducting a risk assessment are possible subsequent actions, but they should be part of the incident response plan. References: 1: Find, lock, or erase a lost Android device - Google Account Help 2: Find, lock, or erase a lost Android device - Android Help 3: Lost or Stolen Mobile Device Procedure - Information Security Office : CISM Practice Quiz | CISM Exam Prep | ISACA : 200 CISM Exam Prep Questions | Free Practice Test | Simplilearn : CISM practice questions to prep for the exam | TechTarget

NEW QUESTION: 146
Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?
A. Requiring challenge/response information
B. Requiring multi factor authentication
C. Enforcing frequent password changes
D. Enforcing complex password formats
Answer: (SHOW ANSWER)
Explanation
Social engineering is a technique used by attackers to manipulate individuals into divulging sensitive information or performing actions that can compromise the security of an organization. Multi-factor authentication (MFA) is a security mechanism that requires users to provide at least two forms of authentication to verify their identity. By requiring MFA, even if an attacker successfully obtains a user's credentials through social engineering, they will not be able to access the network without the additional form of authentication.

NEW QUESTION: 147
Which of the following is MOST important to include in monthly information security reports to the board?
A. Trend analysis of security metrics
B. Risk assessment results
C. Root cause analysis of security incidents
D. Threat intelligence
Answer: (SHOW ANSWER)
Explanation
The most important information to include in monthly information security reports to the board is the trend analysis of security metrics. Security metrics are quantitative and qualitative measures that indicate the

performance and effectiveness of the information security program and the alignment with the business objectives. Trend analysis is the process of comparing and evaluating the changes and patterns of security metrics over time. Trend analysis can help to identify the strengths and weaknesses of the information security program, the progress and achievements of the security goals and initiatives, the gaps and opportunities for improvement, and the impact and value of the information security investments. Trend analysis can also help to communicate the current and future security risks and challenges, and the recommended actions and strategies to address them. Trend analysis can provide the board with a clear and concise overview of the information security status and direction, and enable informed and timely decision making.
References =
CISM Review Manual 15th Edition, page 1631
The CISO's Guide to Reporting Cybersecurity to the Board2
CISM 2020: Information Security Metrics and Reporting, video 13

NEW QUESTION: 148
Which of the following should be established FIRST when implementing an information security governance framework?
A. Security architecture
B. Security policies
C. Security incident management team
D. Security awareness training program
Answer: (SHOW ANSWER)
Explanation
This is the most urgent and effective action to prevent further damage or compromise of the organization's network and data. The other options are less important or irrelevant in this situation.
According to How to identify suspicious insider activity using Active Directory, one of the steps to detect and respond to suspicious activity is to isolate the affected device from the network. This can be done by disabling the network adapter, unplugging the network cable, or blocking the device's IP address on the firewall1. This will prevent the device from communicating with any malicious actors or spreading malware to other devices on the network.
`

NEW QUESTION: 149
Following an employee security awareness training program, what should be the expected outcome?
A. A decrease in the number of viruses detected in incoming emails
B. A decrease in reported social engineering attacks
C. An increase in reported social engineering attempts
D. An increase in user-reported false positive incidents
Answer: (SHOW ANSWER)
Explanation

This outcome indicates that the employees are more aware of the signs and techniques of social engineering and are able to report them to the appropriate authorities. This also helps to prevent successful attacks and reduce the impact of potential breaches.
References: The CISM Review Manual 2023 states that "security awareness training should include information on how to identify and report social engineering attempts" and that "the effectiveness of security awareness training can be measured by the number and quality of reported incidents" (p. 121). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "An increase in reported social engineering attempts is the best indicator that the security awareness training program has been effective, as it shows that the employees are more vigilant and proactive in detecting and reporting such attempts" (p. 45).

NEW QUESTION: 150

Which of the following MUST be defined in order for an information security manager to evaluate the appropriateness of controls currently in place?

A. Security policy
B. Risk management framework
C. Risk appetite
D. Security standards
Answer: (SHOW ANSWER)
Explanation
= Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. It is a key factor that influences the information security strategy and objectives, as well as the selection and implementation of security controls. Risk appetite must be defined in order for an information security manager to evaluate the appropriateness of controls currently in place, as it provides the basis for determining whether the controls are sufficient, excessive, or inadequate to address the risks faced by the organization. The information security manager should align the controls with the risk appetite of the organization, ensuring that the controls are effective, efficient, and economical. References = CISM Review Manual 15th Edition, page 29, page 31.

NEW QUESTION: 151
Which of the following is the BEST indication of a mature information security program?
A. Security incidents are managed properly.
B. Security spending is below budget.
C. Security resources are optimized.
D. Security audit findings are reduced.
Answer: (SHOW ANSWER)
Explanation
A mature information security program is one that is aligned with the business strategy, objectives, and culture, and that delivers value to the organization by effectively managing the information security risks and enhancing the security posture. Optimizing the security resources means that the program uses the available human,

financial, and technical resources in the most efficient and effective way, and that it continuously monitors and improves the performance and maturity of the security processes and controls.
References = CISM Review Manual 2022, page 331; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.22; What is a Mature Information Security Program?; How to Measure the Maturity of Your Cybersecurity Program

NEW QUESTION: 152
An information security program is BEST positioned for success when it is closely aligned with:
A. information security best practices.
B. recognized industry frameworks.
C. information security policies.
D. the information security strategy.
Answer: (SHOW ANSWER)
Explanation
An information security program is best positioned for success when it is closely aligned with the information security strategy, which defines the organization's vision, mission, goals, objectives, and risk appetite for information security. The information security strategy provides the direction and guidance for developing and implementing the information security program, ensuring that it supports the organization's business processes and objectives. The information security strategy also helps to establish the scope, boundaries, roles, responsibilities, and resources for the information security program.
References = CISM Manual, Chapter 3: Information Security Program Development (ISPD), Section 3.1: Information Security Strategy1
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles

NEW QUESTION: 153
Of the following, who is in the BEST position to evaluate business impacts?
A. Senior management
B. Information security manager
C. IT manager
D. Process manager
Answer: (SHOW ANSWER)
Explanation

The process manager is the person who is responsible for overseeing and managing the business processes and functions that are essential for the organization's operations and objectives. The process manager has the most direct and detailed knowledge of the inputs, outputs, dependencies, resources, and performance indicators of the business processes and functions. Therefore, the process manager is in the best position to evaluate the business impacts of a disruption or an incident that affects the availability, integrity, or confidentiality of the information assets and systems that support the business processes and functions. The process manager can identify and quantify the potential losses, damages, or consequences that could result from the disruption or incident, such as revenue loss, customer dissatisfaction, regulatory non-compliance, reputational harm, or legal liability. The process manager can also provide input and feedback to the information security manager and the senior management on the business continuity and disaster recovery plans, the risk assessment and treatment, and the security controls and measures that are needed to protect and recover the business processes and functions. References = CISM Review Manual 15th Edition, page 2301; CISM Practice Quiz, question
1302

NEW QUESTION: 154
An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. What is the information security manager's BEST course of action?
A. Enforce the policy.
B. Modify the policy.
C. Present the risk to senior management.
D. Create an exception for the deviation.
Answer: (SHOW ANSWER)
Explanation
The information security manager's best course of action is to present the risk to senior management, because this is a case of conflicting objectives and priorities between the information security team and the business management. The information security manager should explain the potential impact and likelihood of a security breach due to the violation of the access policy, as well as the possible legal, regulatory, and reputational consequences. The information security manager should also provide alternative solutions that can achieve both operational efficiency and security compliance, such as implementing single sign-on, role-based access control, or multi-factor authentication. The information security manager should not enforce the policy without senior management's approval, because this could cause operational disruption and business dissatisfaction. The information security manager should not modify the policy without a proper risk assessment and approval process, because this could weaken the security posture and expose the organization to more threats. The information security manager should not create an exception for the deviation without a formal risk acceptance and documentation process, because this could create inconsistency and ambiguity in the policy enforcement and accountability. References = CISM Review Manual, 16th Edition, ISACA, 2021, pages 127-128, 138-139, 143-144.

NEW QUESTION: 155

Which of the following would be of GREATEST assistance in determining whether to accept residual risk of a critical security system?

A. Available annual budget

B. Cost-benefit analysis of mitigating controls

C. Recovery time objective (RTO)

D. Maximum tolerable outage (MTO)

Answer: (SHOW ANSWER)

Explanation

Cost-benefit analysis of mitigating controls is the BEST way to assist in determining whether to accept residual risk of a critical security system, because it helps to compare the costs of implementing and maintaining the controls with the benefits of reducing the risk and the potential losses. Cost-benefit analysis can help to justify the investment in security controls and to optimize the level of residual risk that is acceptable for the organization.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 50: "Cost-benefit analysis is the process of comparing the costs of risk treatment options with the benefits of risk reduction and the potential losses from risk events." CISM Review Manual, 16th Edition, ISACA, 2020, p. 51: "Cost-benefit analysis can help to justify the investment in information security controls and to optimize the level of residual risk that is acceptable for the enterprise." CISM Domain 2: Information Risk Management (IRM) [2022 update]: "Cost-benefit analysis: This is a comparison of the costs of implementing and maintaining security controls with the benefits of reducing risk and potential losses. It helps to justify the investment in security controls and optimize the level of residual risk."

NEW QUESTION: 156

Which of the following should be the PRIMARY objective of the information security incident response process?

A. Conducting incident triage

B. Communicating with internal and external parties

C. Minimizing negative impact to critical operations

D. Classifying incidents

Answer: (SHOW ANSWER)

Explanation

The primary objective of the information security incident response process is to minimize the negative impact to critical operations. An information security incident is an event that threatens or compromises the confidentiality, integrity, or availability of the organization's information assets or processes. The information security incident response process is a process that defines the roles, responsibilities, procedures, and tools for detecting, analyzing, containing, eradicating, recovering, and learning from information security incidents. The main goal of the information security incident response process is to restore the normal operations as quickly and effectively as possible, and to prevent or reduce the harm or loss caused by the incident to the organization, its stakeholders, or its environment.

Conducting incident triage (A) is an important activity of the information security incident response process, but not the primary objective. Incident triage is the process of prioritizing and assigning the incidents based on their severity, urgency, and impact. Incident triage helps to allocate the appropriate resources, personnel, and time to handle the incidents, and to escalate the incidents to the relevant authorities or parties if needed. However, incident triage is not the ultimate goal of the information security incident response process, but a means to achieve it.
Communicating with internal and external parties (B) is also an important activity of the information security incident response process, but not the primary objective. Communicating with internal and external parties is the process of informing and updating the stakeholders, such as management, employees, customers, partners, regulators, or media, about the incident status, actions, and outcomes. Communicating with internal and external parties helps to maintain the trust, confidence, and reputation of the organization, and to comply with the legal and contractual obligations, such as notification or reporting requirements. However, communicating with internal and external parties is not the ultimate goal of the information security incident response process, but a means to achieve it.
Classifying incidents (D) is also an important activity of the information security incident response process, but not the primary objective. Classifying incidents is the process of categorizing and labeling the incidents based on their type, source, cause, or impact. Classifying incidents helps to identify and understand the nature and scope of the incidents, and to apply the appropriate response procedures and controls. However, classifying incidents is not the ultimate goal of the information security incident response process, but a means to achieve it.
References = CISM Review Manual, 16th Edition, Chapter 4: Information Security Incident Management, Section: Incident Response Plan, page 1811

NEW QUESTION: 157
An organization is in the process of acquiring a new company Which of the following would be the BEST approach to determine how to protect newly acquired data assets prior to integration?
A. Include security requirements in the contract
B. Assess security controls.
C. Perform a risk assessment
D. Review data architecture.
Answer: (SHOW ANSWER)
Explanation
Performing a risk assessment is the best approach to determine how to protect newly acquired data assets prior to integration, as it will help to identify the threats, vulnerabilities, impacts, and likelihoods of the data assets, and to prioritize the appropriate risk treatment options. Including security requirements in the contract is a good practice, but it may not be sufficient to address the specific risks of the data assets. Assessing security controls and reviewing data architecture are also important steps, but they should be done after performing a risk assessment, as they will depend on the risk level and the risk app The best approach to determine how to protect newly acquired data assets prior to integration is to perform a risk assessment. A risk assessment will identify the various threats and vulnerabilities associated with the data assets and help the organization develop an appropriate security strategy. This risk assessment should include an assessment of the security

controls in place to protect the data, a review of the data architecture, and a review of any contractual requirements related to security.

NEW QUESTION: 158
Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?
A. Intrusion detection
B. Log monitoring
C. Patch management
D. Antivirus software
Answer: (SHOW ANSWER)
Explanation
= Patch management is the process of applying updates to software and hardware systems to fix security vulnerabilities and improve functionality. Patch management is one of the best ways to prevent the exploitation of system vulnerabilities, as it reduces the attack surface and closes the gaps that attackers can exploit. Patch management also helps to ensure compliance with security standards and regulations, and maintain the performance and availability of systems.
Intrusion detection is the process of monitoring network or system activities for signs of malicious or unauthorized behavior. Intrusion detection can help to detect and respond to attacks, but it does not prevent them from happening in the first place. Log monitoring is the process of collecting, analyzing and reviewing log files generated by various systems and applications. Log monitoring can help to identify anomalies, errors and security incidents, but it does not prevent them from occurring. Antivirus software is the program that scans files and systems for viruses, malware and other malicious code. Antivirus software can help to protect systems from infection, but it does not prevent the exploitation of system vulnerabilities that are not related to malware.
Therefore, patch management is the best security process to prevent the exploitation of system vulnerabilities, as it addresses the root cause of the problem and reduces the risk of compromise. References = CISM Review Manual, 16th Edition eBook | Digital | English1, Chapter 4: Information Security Program Development and Management, Section 4.3: Information Security Program Resources, Subsection 4.3.1: Information Security Infrastructure and Architecture, Page 204.

NEW QUESTION: 159
An incident management team is alerted ta a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. notify the business process owner.
B. follow the business continuity plan (BCP).
C. conduct an incident forensic analysis.
D. follow the incident response plan.
Answer: D (LEAVE A REPLY)
Explanation
= Following the incident response plan is the most important step for the security manager before classifying the suspected event as a security incident, as it provides the guidance and procedures for the incident

management team to follow in order to identify, contain, analyze, and resolve security incidents. The incident response plan should define the roles and responsibilities of the incident management team, the criteria and process for incident classification and prioritization, the communication and escalation protocols, the tools and resources for incident handling, and the post-incident review and improvement activities123. References =
1: CISM Review Manual 15th Edition, page 199-2004
2: CISM Practice Quiz, question 1011
3: Computer Security Incident Handling Guide5, page 2-3

NEW QUESTION: 160

Which of the following tools provides an incident response team with the GREATEST insight into insider threat activity across multiple systems?

A. A security information and event management (SIEM) system
B. An intrusion prevention system (IPS)
C. A virtual private network (VPN) with multi-factor authentication (MFA)
D. An identity and access management (IAM) system
Answer: (SHOW ANSWER)
Explanation
A SIEM system is the best tool for providing an incident response team with the greatest insight into insider threat activity across multiple systems because it can collect, correlate, analyze, and report on security events and logs from various sources, such as network devices, servers, applications, and user activities. A SIEM system can also detect and alert on anomalous or suspicious behaviors, such as unauthorized access, data exfiltration, privilege escalation, or policy violations, that may indicate an insider threat. A SIEM system can also support forensic investigations and incident response actions by providing a centralized and comprehensive view of the security posture and incidents.
References: The CISM Review Manual 2023 defines SIEM as "a technology that provides real-time analysis of security alerts generated by network hardware and applications" and states that "SIEM systems can help identify insider threats by correlating user activity logs with other security events and detecting deviations from normal patterns" (p. 184). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "A security information and event management (SIEM) system is the correct answer because it can provide the most insight into insider threat activity across multiple systems by collecting, correlating, analyzing, and reporting on security events and logs from various sources" (p. 95). Additionally, the Detecting and Identifying Insider Threats article from the CISA website states that "threat detection and identification is the process by which persons who might present an insider threat risk due to their observable, concerning behaviors come to the attention of an organization or insider threat team. Detecting and identifying potential insider threats requires both human and technological elements" and that "technological elements include tools such as security information and event management (SIEM) systems, user and entity behavior analytics (UEBA) systems, and data loss prevention (DLP) systems, which can monitor, analyze, and alert on user activities and network events" (p. 1)1.

NEW QUESTION: 161

Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?

A. Inform the public relations officer.

B. Monitor the third party's response.

C. Invoke the incident response plan.

D. Inform customers of the breach.

Answer: (SHOW ANSWER)

Explanation

The first course of action when one of the organization's critical third-party providers experiences a data breach is to invoke the incident response plan, which means activating the incident response team and following the predefined procedures and protocols to respond to the breach. Invoking the incident response plan helps to coordinate the communication and collaboration with the third-party provider, assess the scope and impact of the breach, contain and eradicate the threat, recover the affected systems and data, and report and disclose the incident to the relevant stakeholders and authorities.

References = Cybersecurity Incident Response Exercise Guidance - ISACA, Plan for third-party cybersecurity incident management

NEW QUESTION: 162

Which of the following BEST enables the integration of information security governance into corporate governance?

A. Well-decumented information security policies and standards

B. An information security steering committee with business representation

C. Clear lines of authority across the organization

D. Senior management approval of the information security strategy

Answer: (SHOW ANSWER)

Explanation

= The best way to enable the integration of information security governance into corporate governance is to establish an information security steering committee with business representation. An information security steering committee is a group of senior executives and managers from different business units and functions who are responsible for overseeing, directing, and supporting the information security program and strategy of the organization. An information security steering committee with business representation can enable the integration of information security governance into corporate governance by providing the following benefits12:

Align the information security objectives and priorities with the business objectives and priorities, and ensure that the information security program and strategy support and enable the achievement of the organizational goals and performance.

Communicate and promote the value and importance of information security to the board of directors, senior management, and other stakeholders, and ensure that information security is considered and incorporated in the decision making and planning processes of the organization.

Provide guidance and direction to the information security manager and the information security team, and ensure that they have the necessary authority, resources, and support to implement and maintain the information security program and strategy effectively and efficiently.

Monitor and evaluate the performance and outcomes of the information security program and strategy, and ensure that they are aligned with the expectations and requirements of the organization and its stakeholders, as well as the relevant laws, regulations, standards, and best practices.
Identify and address the issues, challenges, and opportunities related to information security, and ensure that the information security program and strategy are continuously improved and updated to reflect the changes and developments in the internal and external environment.
The other options are not the best way to enable the integration of information security governance into corporate governance, as they are less comprehensive, effective, or influential than establishing an information security steering committee with business representation. Well-documented information security policies and standards are important components of the information security program and strategy, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not reflect or align with the business needs, priorities, or expectations, and they may not be communicated, implemented, or enforced properly or consistently across the organization. Clear lines of authority across the organization are important factors for the information security governance structure, but they are not sufficient to enable the integration of information security governance into corporate governance, as they may not ensure the involvement, participation, or support of the senior executives, managers, and other stakeholders who are responsible for or affected by information security. Senior management approval of the information security strategy is an important outcome of the information security governance process, but it is not sufficient to enable the integration of information security governance into corporate governance, as it may not ensure the alignment, communication, or monitoring of the information security strategy with the business strategy, and it may not ensure the accountability, responsibility, or authority of the information security manager and the information security team12. References = CISM Domain 1: Information Security Governance (ISG) [2022 update], Information Security Governance for CISM | Pluralsight, Aligning Information Security with Business Strategy - ISACA, Aligning Information Security with Business Objectives - ISACA

NEW QUESTION: 163
Which of the following should be the PRIMARY basis for a severity hierarchy for information security incident classification?
A. Availability of resources
B. Root cause analysis results
C. Adverse effects on the business
D. Legal and regulatory requirements
Answer: (SHOW ANSWER)
Explanation
The severity hierarchy for information security incident classification should be based on the potential or actual impact of the incident on the business objectives, operations, reputation, and stakeholders. The adverse effects on the business can be measured by criteria such as financial loss, operational disruption, legal liability, regulatory compliance, customer satisfaction, and public confidence. The other options are not the primary basis for a severity hierarchy, although they may be considered as secondary factors or consequences of an incident

NEW QUESTION: 164
Which of the following would be MOST useful when determining the business continuity strategy for a large organization's data center?
A. Stakeholder feedback analysis
B. Business continuity risk analysis
C. Incident root cause analysis
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
Explanation
According to the CISM Review Manual, a business impact analysis (BIA) is the most useful tool when determining the business continuity strategy for a large organization's data center, as it helps to identify and prioritize the critical business processes and resources that depend on the data center, and the impact of their disruption or loss. A BIA also provides the basis for defining the recovery time objectives (RTOs) and recovery point objectives (RPOs) for the data center, which guide the selection of the appropriate business continuity strategy.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.5.2, page 1511.

NEW QUESTION: 165
Which of the following factors has the GREATEST influence on the successful implementation of information security strategy goals?
A. Regulatory requirements
B. Compliance acceptance
C. Management support
D. Budgetary approval
Answer: C (LEAVE A REPLY)
Explanation
Management support is the factor that has the greatest influence on the successful implementation of information security strategy goals. Management support refers to the commitment and involvement of senior executives and other key stakeholders in defining, approving, funding, and overseeing the information security strategy. Management support is essential for aligning the information security strategy with the business objectives, ensuring adequate resources and budget, fostering a security-aware culture, and enforcing accountability and compliance. According to ISACA, management support is one of the critical success factors for information security governance1. The other options are not factors that influence the successful implementation of information security strategy goals, but rather outcomes or components of the information security strategy. Regulatory requirements are external obligations that the information security strategy must comply with2. Compliance acceptance is the degree to which the organization adheres to the information security policies and standards3. Budgetary approval is the process of allocating financial resources for the information security activities and initiatives4. References: 2: Information Security: Goals, Types and Applications - Exabeam 3: How to develop a cybersecurity strategy: Step-by-step guide 4: Information Security Goals And Objectives 1: The Importance of Building an Information Security Strategic Plan

NEW QUESTION: 166
Which of the following would be MOST useful to help senior management understand the status of information security compliance?
A. Industry benchmarks
B. Key performance indicators (KPIs)
C. Business impact analysis (BIA) results
D. Risk assessment results
Answer: (SHOW ANSWER)
Explanation
Key performance indicators (KPIs) are measurable values that demonstrate how effectively an organization is achieving its key objectives and goals. KPIs can help senior management understand the status of information security compliance by providing quantifiable and relevant data on the performance and progress of the information security program and processes. KPIs can also help senior management to evaluate the effectiveness and efficiency of the information security controls and activities, identify strengths and weaknesses, and make informed decisions and adjustments. KPIs should be aligned with the organization's strategy, vision, and mission, and should be SMART (specific, measurable, achievable, relevant, and time-bound). Some examples of information security KPIs are: percentage of compliance with policies and standards, number of security incidents and breaches, mean time to detect and respond to incidents, percentage of systems and applications patched, number of security awareness trainings completed, etc. Industry benchmarks, business impact analysis (BIA) results, and risk assessment results are not the most useful to help senior management understand the status of information security compliance, although they may provide some useful information or insights. Industry benchmarks are comparative measures of the performance or practices of other organizations in the same industry or sector. Industry benchmarks can help senior management to compare and contrast their own information security performance or practices with those of their peers or competitors, and identify gaps or opportunities for improvement. However, industry benchmarks may not reflect the specific goals, needs, or context of the organization, and may not be readily available or reliable. Business impact analysis (BIA) results are the outcomes of the process of analyzing the potential impacts of disruptive events on the organization's critical business functions and processes. BIA results can help senior management to understand the dependencies, priorities, and recovery objectives of the organization's business functions and processes, and to plan for business continuity and disaster recovery. However, BIA results do not directly measure or indicate the status of information security compliance, and may not be updated or accurate. Risk assessment results are the outcomes of the process of identifying, analyzing, and evaluating the information security risks that the organization faces. Risk assessment results can help senior management to understand the sources, causes, and consequences of information security risks, and to determine the appropriate risk responses and controls. However, risk assessment results do not directly measure or indicate the status of information security compliance, and may vary depending on the risk assessment methodology, criteria, and frequency. References = CISM Review Manual, 16th Edition, pages 47-481, 54-551, 69-701, 72-731; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 832 Key performance indicators (KPIs) are metrics that measure the effectiveness and ef-ficiency of information security processes and activities. They help senior manage-ment understand the status of information security compliance by providing relevant, timely and accurate information on the performance of

security controls, the level of risk exposure, the return on security investment and the progress toward security ob-jectives. KPIs can also be used to benchmark the organization's security performance against industry standards or best practices. KPIs should be aligned with the organiza-tion's strategic goals and risk appetite, and should be reported regularly to senior man-agement and other stakeholders.
References:
*1 Key Performance Indicators for Security Governance, Part 1 - ISACA
*2 Key Performance Indicators for Security Governance, Part 2 - ISACA
*3 Compliance Metrics and KPIs For Measuring Compliance Effectiveness - Reciprocity
*4 14 Cybersecurity Metrics + KPIs You Must Track in 2023 - UpGuard

NEW QUESTION: 167
When deciding to move to a cloud-based model, the FIRST consideration should be:
A. storage in a shared environment.
B. availability of the data.
C. data classification.
D. physical location of the data.
Answer: C (LEAVE A REPLY)
Explanation
The first consideration when deciding to move to a cloud-based model should be data classification, because it helps the organization to identify the sensitivity, value, and criticality of the data that will be stored, processed, or transmitted in the cloud. Data classification can help the organization to determine the appropriate level of protection, encryption, and access control for the data, and to comply with the relevant legal, regulatory, and contractual requirements. Data classification can also help the organization to evaluate the suitability, compatibility, and trustworthiness of the cloud service provider and the cloud service model, and to negotiate the terms and conditions of the cloud service contract.
Storage in a shared environment, availability of the data, and physical location of the data are all important considerations when deciding to move to a cloud-based model, but they are not the first consideration. Storage in a shared environment can affect the security, privacy, and integrity of the data, as the data may be co-located with other customers' data, and may be subject to unauthorized access, modification, or deletion. Availability of the data can affect the reliability, performance, and continuity of the data, as the data may be inaccessible, corrupted, or lost due to network failures, service outages, or disasters. Physical location of the data can affect the compliance, sovereignty, and jurisdiction of the data, as the data may be stored or transferred across different countries or regions, and may be subject to different laws, regulations, or policies.

However, these considerations depend on the data classification, as different types of data may have different levels of risk, impact, and expectation in the cloud environment. References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 95-96, 99-100, 103-104, 107-108.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1031.

NEW QUESTION: 168
Which of the following would be an information security managers PRIMARY challenge when deploying a bring your own device (BYOD) mobile program in an enterprise?
A. Mobile application control
B. Inconsistent device security
C. Configuration management
D. End user acceptance
Answer: (SHOW ANSWER)
Explanation
Inconsistent device security is the primary challenge for an information security manager when deploying a bring your own device (BYOD) mobile program in an enterprise because it increases the risk of data breaches and compromises. A BYOD mobile program allows employees to use their personal devices, such as smartphones, tablets, or laptops, to access the organization's network, applications, and data. However, personal devices may have different operating systems, versions, configurations, and security settings than the organization's standard devices. Moreover, personal devices may not be updated regularly, may have unauthorized or malicious apps installed, or may not have adequate protection against malware or theft. Inconsistent device security makes it difficult for the information security manager to enforce and monitor the security policies and controls across all devices, as well as to ensure compliance with the regulatory requirements for data privacy and security. Therefore, inconsistent device security is the correct answer.
References:
* https://simplemdm.com/blog/challenges-of-bring-your-own-device-byod-policy/
* https://www.timedoctor.com/blog/byod-pros-and-cons/
* https://www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf

NEW QUESTION: 169
Which of the following is the MOST essential element of an information security program?
A. Benchmarking the program with global standards for relevance
B. Prioritizing program deliverables based on available resources
C. Involving functional managers in program development
D. Applying project management practices used by the business
Answer: (SHOW ANSWER)
Explanation
Involving functional managers in program development is the most essential element of an information security program, because they are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units. They also provide input and

feedback on the information security requirements, risks, and controls that affect their operations and objectives.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Functional managers are responsible for ensuring that the information security policies, standards, and procedures are implemented and enforced within their respective business units." CISM Review Manual, 16th Edition, ISACA, 2020, p. 38: "Functional managers should be involved in the development of the information security program to provide input and feedback on the information security requirements, risks, and controls that affect their operations and objectives."

NEW QUESTION: 170

Following a risk assessment, an organization has made the decision to adopt a bring your own device (BYOD) strategy. What should the information security manager do NEXT?

A. Develop a personal device policy
B. Implement a mobile device management (MDM) solution
C. Develop training specific to BYOD awareness
D. Define control requirements
Answer: (SHOW ANSWER)
Explanation
Defining control requirements is the next step to ensure the security policy framework encompasses the new business model because it is a process of identifying and specifying the security measures and standards that are needed to protect the data and applications accessed by the BYOD devices. Defining control requirements helps to establish the baseline security level and expectations for the BYOD strategy, as well as to align them with the business objectives and risks. Therefore, defining control requirements is the correct answer.
References:
https://www.digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effec
https://learn.microsoft.com/en-us/mem/intune/fundamentals/byod-technology-decisions

NEW QUESTION: 171
Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?
A. Disaster recovery plan (DRP)
B. Incident response plan
C. Business continuity plan (BCP)
D. Business contingency plan
Answer: (SHOW ANSWER)
Explanation
= A business continuity plan (BCP) is the plan that should be invoked by an organization in an effort to remain operational during a disaster. A disaster is a sudden, unexpected, or disruptive event that causes significant damage, loss, or interruption to the organization's normal operations, assets, or resources. Examples of disasters are natural disasters, such as earthquakes, floods, or fires, or human-made disasters, such as cyberattacks, sabotage, or terrorism. A BCP is a document that describes the procedures, strategies, and

actions that the organization will take to ensure the continuity of its critical business functions, processes, and services in the event of a disaster. A BCP also defines the roles and responsibilities of the staff, management, and other stakeholders involved in the business continuity management, and the resources, tools, and systems that will support the business continuity activities. A BCP helps the organization to:
Minimize the impact and duration of the disaster on the organization's operations, assets, and reputation.
Restore the essential functions and services as quickly and efficiently as possible.
Protect the health, safety, and welfare of the staff, customers, and partners.
Meet the legal, regulatory, contractual, and ethical obligations of the organization.
Learn from the disaster and improve the business continuity capabilities and readiness of the organization.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Business Continuity Plan (BCP), page 1771; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 83, page 772.

NEW QUESTION: 172
Data entry functions for a web-based application have been outsourced to a third-party service provider who will work from a remote site Which of the following issues would be of GREATEST concern to an information security manager?
A. The application does not use a secure communications protocol
B. The application is configured with restrictive access controls
C. The business process has only one level of error checking
D. Server-based malware protection is not enforced
Answer: (SHOW ANSWER)
Explanation
Server-based malware protection is not enforced is the issue that would be of GREATEST concern to an information security manager, as it exposes the web-based application and its data to potential threats from malicious software that can compromise the confidentiality, integrity, and availability of the information. Server-based malware protection is a security control that monitors and blocks malicious activities on the server where the application runs, such as viruses, worms, trojans, ransomware, etc. Without server-based malware protection, the web-based application may be vulnerable to attacks that can damage or destroy the data stored on the server, or disrupt the normal functioning of the application. The other issues are also important, but not as critical as server-based malware protection. The application does not use a secure communications protocol may expose sensitive data in transit to eavesdropping or interception by unauthorized parties. The application is configured with restrictive access controls may limit the access rights of legitimate users to authorized resources, but it does not prevent unauthorized users from accessing them through other means. The business process has only one level of error checking may result in incorrect or inconsistent data entry or processing, but it does not guarantee data quality or accuracy. References = CISM Review Manual, 16th Edition, page 1751; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 812

NEW QUESTION: 173

An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident. Which of the following should the information security manager do FIRST?

A. Set up communication channels for the target audience.

B. Determine the needs and requirements of each audience.

C. Create a comprehensive singular communication

D. Invoke the organization's incident response plan.

Answer: (SHOW ANSWER)

Explanation

The information security manager should do FIRST invoke the organization's incident response plan, which is a predefined set of procedures and guidelines for handling security incidents in a timely and effective manner. The incident response plan should include the roles and responsibilities of the incident response team, the communication protocols and channels, the escalation and reporting procedures, and the documentation and evidence collection requirements. By invoking the incident response plan, the information security manager can ensure that the incident is properly contained, analyzed, resolved, and reported, and that the appropriate stakeholders are informed and involved. The other options are not the first actions that the information security manager should take, as they are part of the communication process that follows the incident response plan. Setting up communication channels for the target audience, determining the needs and requirements of each audience, and creating a comprehensive singular communication are all important steps for communicating effectively with the board, regulatory agencies, and the media, but they are not the first priority in the event of a security incident. The information security manager should first follow the incident response plan to manage the incident and its impact, and then communicate the relevant information to the target audience according to the plan. References = CISM Review Manual, 16th Edition, page 2261; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1012 Determining the needs and requirements of each audience should be the FIRST step in developing materials to update the board, regulatory agencies, and the media about a security incident. This is because different audiences have different expectations, interests, and concerns regarding the incident and its impact. By understanding the needs and requirements of each audience, the information security manager can tailor the communication materials to address them effectively and appropriately. This will also help to avoid confusion, misinformation, or misinterpretation of the incident details and response actions

NEW QUESTION: 174

An international organization with remote branches is implementing a corporate security policy for managing personally identifiable information (PII). Which of the following should be the information security manager's MAIN concern?

A. Local regulations

B. Data backup strategy

C. Consistency in awareness programs

D. Organizational reporting structure

Answer: (SHOW ANSWER)

Explanation

Local regulations are the main concern for the information security manager when implementing a corporate security policy for managing PII, as different countries or regions may have different legal, regulatory or contractual requirements for the protection, processing, storage and transfer of PII. The information security manager should ensure that the policy complies with the applicable local regulations and respects the rights and preferences of the data subjects. The policy should also address the risks and challenges of cross-border data transfers and the use of cloud services.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2191; CISM Online Review Course, Module 4, Lesson 2, Topic 12; Comparitech, PII Compliance: What is it and How to Implement it3

NEW QUESTION: 175
Which of the following is the BEST course of action if the business activity residual risk is lower than the acceptable risk level?
A. Monitor the effectiveness of controls
B. Update the risk assessment framework
C. Review the inherent risk level
D. Review the risk probability and impact
Answer: (SHOW ANSWER)
Explanation
If the residual risk of the business activity is lower than the acceptable risk level, it means that the existing controls are effectively mitigating the identified risks. In this case, the best course of action is to monitor the effectiveness of the controls and ensure they remain effective. The information security manager should review and test the controls periodically to ensure that they continue to provide adequate protection. It is also essential to update the risk assessment framework to reflect changes in the business environment or risk landscape.

NEW QUESTION: 176
Which of the following should be the PRIMARY area of focus when mitigating security risks associated with emerging technologies?
A. Compatibility with legacy systems
B. Application of corporate hardening standards
C. Integration with existing access controls
D. Unknown vulnerabilities
Answer: (SHOW ANSWER)
Explanation
= The primary area of focus when mitigating security risks associated with emerging technologies is unknown vulnerabilities. Emerging technologies are new and complex, and often involve multiple parties, interdependencies, and uncertainties. Therefore, they may have unknown vulnerabilities that could expose the organization to threats that are difficult to predict, detect, or prevent1. Unknown vulnerabilities could also result from the lack of experience, knowledge, or best practices in implementing, operating, or securing emerging technologies2. Unknown vulnerabilities could lead to serious consequences, such as data breaches, system failures, reputational damage, legal liabilities, or regulatory sanctions3. Therefore, it is important to focus on

identifying, assessing, and addressing unknown vulnerabilities when mitigating security risks associated with emerging technologies.
The other options are not as important as unknown vulnerabilities, because they are either more predictable, manageable, or specific. Compatibility with legacy systems is a technical issue that could affect the performance, functionality, or reliability of emerging technologies, but it is not a security risk per se. It could be resolved by testing, upgrading, or replacing legacy systems4. Application of corporate hardening standards is a security measure that could reduce the attack surface and improve the resilience of emerging technologies, but it is not a sufficient or comprehensive solution. It could be limited by the availability, applicability, or effectiveness of the standards. Integration with existing access controls is a security requirement that could prevent unauthorized or inappropriate access to emerging technologies, but it is not a guarantee of security. It could be challenged by the complexity, diversity, or dynamism of the access scenarios. References = 1: Performing Risk Assessments of Emerging Technologies - ISACA 2: Assessing the Risk of Emerging Technology - ISACA 3: Factors Influencing Public Risk Perception of Emerging Technologies: A ... 4: CISM Review Manual 15th Edition, Chapter 3, Section 3.3 : CISM Review Manual 15th Edition, Chapter 3, Section 3.4 : CISM Review Manual 15th Edition, Chapter 3, Section 3.5

NEW QUESTION: 177
Which of the following is MOST important to include in an information security status report management?
A. List of recent security events
B. Key risk indication (KRIs)
C. Review of information security policies
D. information security budget requests
Answer: (SHOW ANSWER)
Explanation
Key risk indicators (KRIs) are the most useful to include in an information security status report for management because they measure and report the level of risk exposure or performance against predefined risk thresholds or targets, and alert management of any deviations or issues that may require attention or action. List of recent security events is not very useful to include in an information security status report for management because it does not provide any analysis or evaluation of the events or their impact on the organization's objectives or performance. Review of information security policies is not very useful to include in an information security status report for management because it does not reflect any progress or results of implementing or enforcing the policies. Information security budget requests are not very useful to include in an information security status report for management because they do not indicate any value or benefit of investing in information security initiatives or controls. References:
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-inform

NEW QUESTION: 178
When drafting the corporate privacy statement for a public website, which of the following MUST be included?
A. Limited liability clause
B. Explanation of information usage

C. Information encryption requirements
D. Access control requirements
Answer: (SHOW ANSWER)
Explanation
A privacy statement should inform the users of the website how their personal information will be collected, used, shared, and protected by the organization. References = CISM Review Manual, 16th Edition, Chapter 4, Section 4.2.1.11

NEW QUESTION: 179
Which of the following would be MOST helpful when creating information security policies?
A. The information security framework
B. Business impact analysis (BIA)
C. Information security metrics
D. Risk assessment results
Answer: (SHOW ANSWER)
Explanation
The information security framework is a set of principles, standards, guidelines, and best practices that define the scope, objectives, and requirements for information security in an organization. The information security framework is most helpful when creating information security policies because it provides a consistent and coherent approach to managing information security risks, aligning with business goals and strategy, and complying with relevant laws and regulations. The information security framework also helps to establish the roles, responsibilities, and accountability of all stakeholders involved in information security governance, management, and operations.
References = CISM Manual1, Chapter 3: Information Security Program Development (ISPD), Section 3.1: Information Security Framework2
1: https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles 2: 1

NEW QUESTION: 180
Which of the following is MOST important to consider when choosing a shared alternate location for computing facilities?

A. The organization's risk tolerance
B. Resource availability
C. The organization's mission
D. Incident response team training
Answer: (SHOW ANSWER)
Explanation
The organization's risk tolerance is the most important factor to consider when choosing a shared alternate location for computing facilities, because it determines the acceptable level of risk exposure and the required recovery time objectives (RTOs) and recovery point objectives (RPOs) for the organization's critical business processes and information assets. Resource availability, the organization's mission, and incident response team training are also important considerations, but they are secondary to the risk tolerance.

References = CISM Review Manual, 16th Edition, page 290

NEW QUESTION: 181
Which of the following has The GREATEST positive impact on The ability to execute a disaster recovery plan (DRP)?
A. Storing the plan at an offsite location
B. Communicating the plan to all stakeholders
C. Updating the plan periodically
D. Conducting a walk-through of the plan
Answer: (SHOW ANSWER)
Explanation
A walk-through of the disaster recovery plan (DRP) is a method of testing the plan by simulating a disaster scenario and having the participants review their roles and responsibilities, as well as the procedures and resources required to execute the plan. A walk-through has the greatest positive impact on the ability to execute the DRP, as it helps to identify and resolve any gaps, errors, or inconsistencies in the plan, as well as to enhance the awareness and readiness of the stakeholders involved in the recovery process. References = CISM Review Manual, 16th Edition, Chapter 5, Section 5.3.2.21

NEW QUESTION: 182
Which of the following metrics provides the BEST evidence of alignment of information security governance with corporate governance?
A. Average return on investment (ROI) associated with security initiatives
B. Average number of security incidents across business units
C. Mean time to resolution (MTTR) for enterprise-wide security incidents
D. Number of vulnerabilities identified for high-risk information assets
Answer: (SHOW ANSWER)
Explanation
Average return on investment (ROI) associated with security initiatives is the best metric to provide evidence of alignment of information security governance with corporate governance because it demonstrates the value and benefits of security investments to the organization's strategic goals and objectives. Average number of security incidents across business units is not a good metric because it does not measure the effectiveness or efficiency of security initiatives or their alignment with corporate governance. Mean time to resolution (MTTR) for enterprise-wide security incidents is not a good metric because it does not measure the impact or outcome

of security initiatives or their alignment with corporate governance. Number of vulnerabilities identified for high-risk information assets is not a good metric because it does not measure the performance or improvement of security initiatives or their alignment with corporate governance. References:
https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/measuring-the-value-of-information-securit
https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the-effectiveness-of-inform

NEW QUESTION: 183
Which of the following will provide the MOST guidance when deciding the level of protection for an information asset?
A. Impact on information security program
B. Cost of controls
C. Impact to business function
D. Cost to replace
Answer: (SHOW ANSWER)
Explanation
The level of protection for an information asset should be based on the impact to the business function that depends on the asset. The impact to the business function reflects the value and criticality of the information asset to the organization, and the potential consequences of its loss, compromise, or unavailability. The impact to the business function can be measured in terms of financial, operational, reputational, legal, or strategic effects. The higher the impact, the higher the level of protection required.
Impact on information security program, cost of controls, and cost to replace are not the best factors to provide guidance when deciding the level of protection for an information asset. Impact on information security program is a secondary effect that depends on the impact to the business function. Cost of controls and cost to replace are important considerations for implementing and maintaining the protection, but they do not determine the level of protection needed. Cost of controls and cost to replace should be balanced with the impact to the business function and the risk appetite of the organization. References = CISM Certified Information Security Manager Study Guide, Chapter 2: Information Risk Management, page 671; CISM Foundations: Module 2 Course, Part One: Information Risk Management2; CISM Review Manual 15th Edition, Chapter 2: Information Risk Management, page 693 When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture.
Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when determining the appropriate level of protection for the asset.

NEW QUESTION: 184
Which of the following is the PRIMARY reason to monitor key risk indicators (KRIs) related to information security?

A. To alert on unacceptable risk
B. To identify residual risk
C. To reassess risk appetite
D. To benchmark control performance
Answer: (SHOW ANSWER)
Explanation
Key risk indicators (KRIs) are metrics that measure the level of risk exposure and the likelihood of occurrence of potential adverse events that can affect the organization's objectives and performance. KRIs are used to monitor changes in the risk environment and to provide early warning signals for potential issues that may require management attention or intervention. KRIs are also used to communicate the risk status and trends to the relevant stakeholders and to support risk-based decision making12.
The primary reason to monitor KRIs related to information security is to alert on unacceptable risk. Unacceptable risk is the level of risk that exceeds the organization's risk appetite, tolerance, or threshold, and that poses a significant threat to the organization's assets, operations, reputation, or compliance. Unacceptable risk can result from internal or external factors, such as cyberattacks, data breaches, system failures, human errors, fraud, natural disasters, or regulatory changes. Unacceptable risk can have severe consequences for the organization, such as financial losses, legal liabilities, operational disruptions, customer dissatisfaction, or reputational damage12.
By monitoring KRIs related to information security, the organization can identify and assess the sources, causes, and impacts of unacceptable risk, and take timely and appropriate actions to mitigate, transfer, avoid, or accept the risk. Monitoring KRIs can also help the organization to evaluate the effectiveness and efficiency of the existing information security controls, policies, and procedures, and to identify and implement any necessary improvements or enhancements. Monitoring KRIs can also help the organization to align its information security strategy and objectives with its business strategy and objectives, and to ensure compliance with the relevant laws, regulations, standards, and best practices12.
While monitoring KRIs related to information security can also serve other purposes, such as identifying residual risk, reassessing risk appetite, or benchmarking control performance, these are not the primary reason for monitoring KRIs. Residual risk is the level of risk that remains after applying the risk treatment options, and it should be within the organization's risk appetite, tolerance, or threshold. Reassessing risk appetite is the process of reviewing and adjusting the amount and type of risk that the organization is willing to take in pursuit of its objectives, and it should be done periodically or when there are significant changes in the internal or external environment. Benchmarking control performance is the process of comparing the organization's information security controls with those of other organizations or industry standards, and it should be done to identify and adopt the best practices or to demonstrate compliance12. References = Integrating KRIs and KPIs for Effective Technology Risk Management, The Power of KRIs in Enterprise Risk Management (ERM) - Metricstream, What Is a Key Risk Indicator? With Characteristics and Tips, KRI Framework for Operational Risk Management | Workiva, Key risk indicator - Wikipedia

NEW QUESTION: 185
An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:

* A bad actor broke into a business-critical FTP server by brute forcing an administrative password
* The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
* The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
* After three hours, the bad actor deleted the FTP directory, causing incoming FTP attempts by legitimate customers to fail Which of the following could have been prevented by conducting regular incident response testing?

A. Ignored alert messages
B. The server being compromised
C. The brute force attack
D. Stolen data
Answer: (SHOW ANSWER)
Explanation
Ignored alert messages could have been prevented by conducting regular incident response testing because it would have ensured that the help desk staff are familiar with and trained on how to handle different types of alert messages from different sources, and how to escalate them appropriately. The server being compromised could not have been prevented by conducting regular incident response testing because it is related to security vulnerabilities or weaknesses in the server configuration or authentication mechanisms. The brute force attack could not have been prevented by conducting regular incident response testing because it is related to security threats or attacks from external sources. Stolen data could not have been prevented by conducting regular incident response testing because it is related to security breaches or incidents that may occur despite the incident response plan or process. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/incident-response-lessons-learned

NEW QUESTION: 186
When developing an asset classification program, which of the following steps should be completed FIRST?
A. Categorize each asset.
B. Create an inventory. &
C. Create a business case for a digital rights management tool.
D. Implement a data loss prevention (OLP) system.
Answer: B (LEAVE A REPLY)
Explanation
Creating an inventory is the FIRST step in developing an asset classification program because it helps to identify and list all the information systems assets of the organization that need to be protected and classified. An inventory should include the asset name, description, owner, custodian, location, type, value, and other relevant attributes. Creating an inventory also enables the establishment of the ownership and custody of the assets, which are essential for defining the roles and responsibilities for asset protection and classification12. Categorizing each asset (A) is a subsequent step in developing an asset classification program, after creating an inventory. Categorizing each asset involves assigning a security level or category to each asset based on

its value, sensitivity, and criticality to the organization. The security level or category determines the protection level and controls required for each asset12. Creating a business case for a digital rights management tool is not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A digital rights management tool is a type of control that can help to enforce the security policies and objectives for the classified assets, such as preventing unauthorized access, copying, or distribution of the assets3. Implementing a data loss prevention (DLP) system (D) is also not a step in developing an asset classification program, but rather a possible outcome or recommendation based on the asset classification results. A DLP system is a type of control that can help to monitor, detect, and prevent the loss or leakage of the classified assets, such as through email, web, or removable media4. References = 1: CISM Review Manual 15th Edition, page 77-781; 2: IT Asset Valuation, Risk Assessment and Control Implementation Model - ISACA2; 3: What is Digital Rights Management? - Definition from Techopedia3; 4: What is Data Loss Prevention (DLP)? - Definition from Techopedia4

NEW QUESTION: 187
Which of the following is MOST important to consider when determining asset valuation?
A. Asset recovery cost
B. Asset classification level
C. Cost of insurance premiums
D. Potential business loss
Answer: (SHOW ANSWER)
Explanation
Potential business loss is the most important factor to consider when determining asset valuation, as it reflects the impact of losing or compromising the asset on the organization's objectives and operations. Asset recovery cost, asset classification level, and cost of insurance premiums are also relevant, but not as important as potential business loss, as they do not capture the full value of the asset to the organization. References = CISM Review Manual 2023, page 461; CISM Review Questions, Answers & Explanations Manual 2023, page 292

NEW QUESTION: 188
A new application has entered the production environment with deficient technical security controls. Which of the following is MOST Likely the root cause?
A. Inadequate incident response controls
B. Lack of legal review
C. Inadequate change control
D. Lack of quality control
Answer: (SHOW ANSWER)
Explanation
Change control is the process of ensuring that changes to an information system are authorized, tested, documented and implemented in a controlled manner. Inadequate change control can result in deficient technical security controls, such as missing patches, misconfigurations, vulnerabilities or errors in the new application.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.3.2, page 2291

NEW QUESTION: 189
Which of the following is the PRIMARY role of the information security manager in application development?
A. To ensure security is integrated into the system development life cycle (SDLC)
B. To ensure compliance with industry best practice
C. To ensure enterprise security controls are implemented
D. To ensure control procedures address business risk
Answer: (SHOW ANSWER)
Explanation
According to the CISM Review Manual, one of the primary roles of the information security manager in application development is to ensure that security is integrated into the SDLC. This means that security requirements, design, testing, deployment, and maintenance are all considered and addressed throughout the application development process. By doing so, the information security manager can help to prevent or mitigate security risks, ensure compliance with standards and regulations, and improve the quality and reliability of the application1 The other options are not as accurate as ensuring security is integrated into the SDLC. Ensuring compliance with industry best practices is a secondary role of the information security manager in application development, as it involves following established guidelines and frameworks for secure application development. However, compliance alone does not guarantee that security is actually implemented in the application. Ensuring enterprise security controls are implemented is a tertiary role of the information security manager in application development, as it involves applying existing policies and procedures for managing and monitoring security activities across the organization. However, enterprise controls alone do not ensure that security is tailored to the specific needs and context of each application. Ensuring control procedures address business risk is a quaternary role of the information security manager in application development, as it involves identifying and assessing potential threats and vulnerabilities that could affect the business objectives and operations of each application. However, business risk alone does not ensure that security measures are aligned with the value proposition and benefits of each application1 References = 1: CISM Review Manual, 16th Edition, ISACA, 2020, pp. 30-31...

NEW QUESTION: 190
Which of the following is the MOST important issue in a penetration test?
A. Having an independent group perform the test
B. Obtaining permission from audit
C. Performing the test without the benefit of any insider knowledge
D. Having a defined goal as well as success and failure criteria
Answer: (SHOW ANSWER)
Explanation
The most important issue in a penetration test is having a defined goal as well as success and failure criteria. A penetration test is a simulated cyber attack against a computer system or an application to check for exploitable vulnerabilities. The goal of a penetration test is to identify and evaluate the security risks and weaknesses of the target system or application, and to provide recommendations for improvement. The

success and failure criteria of a penetration test are the metrics and indicators that measure the effectiveness and efficiency of the test, and the extent to which the test achieves its goal. By having a defined goal as well as success and failure criteria, the penetration tester can plan and execute the test in a systematic and structured manner, and can communicate and report the results and findings in a clear and concise way. The other options are not the most important issue in a penetration test, although they may be some factors or considerations that affect the test. Having an independent group perform the test is a desirable practice, as it can provide an unbiased and objective assessment of the target system or application. However, it is not essential, as long as the penetration tester follows ethical hacking principles and standards. Obtaining permission from audit is a mandatory requirement, as it ensures that the penetration test is authorized and compliant with the organization's policies and regulations. However, it is not an issue, as it is a prerequisite for conducting the test. Performing the test without the benefit of any insider knowledge is an optional approach, as it simulates a real-world attack by an external hacker who does not have access to the internal design or configuration of the target system or application. However, it is not always feasible or effective, as some vulnerabilities may be hidden or inaccessible from an outsider's perspective.

NEW QUESTION: 191
Which of the following is the BEST way to determine if an information security profile is aligned with business requirements?
A. Review the key performance indicator (KPI) dashboard
B. Review security-related key risk indicators (KRIs)
C. Review control self-assessment (CSA) results
D. Review periodic security audits
Answer: (SHOW ANSWER)
Explanation
Security-related KRIs are metrics that measure the effectiveness of the information security profile in achieving the business objectives and managing the risks. Reviewing security-related KRIs can help to determine if the information security profile is aligned with business requirements, as they reflect the security performance and outcomes that are relevant for the business. Reviewing other options, such as KPIs, CSAs, or audits, may provide some insights into the security status, but they are not the best way to assess the alignment with business requirements, as they may not capture the business context and goals adequately. References:
* https://www.nist.gov/cyberframework/examples-framework-profiles
* https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/accountability-for-information-securi
* https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea-top-d

NEW QUESTION: 192
Which of the following has the MOST influence on the inherent risk of an information asset?
A. Risk tolerance
B. Net present value (NPV)
C. Return on investment (ROI)
D. Business criticality
Answer: (SHOW ANSWER)

Explanation
Inherent risk is the risk that exists before any controls are applied. It is influenced by factors such as the nature, value, sensitivity, and exposure of the information asset. Business criticality is one of the most important factors that affect the inherent risk of an information asset, as it reflects how essential the asset is for the organization's operations and objectives. The higher the business criticality, the higher the inherent risk. Risk tolerance, NPV, and ROI are not directly related to the inherent risk of an information asset, as they are more relevant for the risk assessment and risk treatment processes. References = CISM Review Manual, 16th Edition, page 971Business criticality is the degree to which an asset is essential to the success of the business and the extent to which its loss or compromise could have a significant impact on the business. Business criticality is one of the main factors that help to determine the inherent risk of an asset, as assets that are more critical to the business tend to have a higher inherent risk.

NEW QUESTION: 193
Which of the following is the GREATEST benefit of information asset classification?
A. Helping to determine the recovery point objective (RPO)
B. Providing a basis for implementing a need-to-know policy
C. Supporting segregation of duties
D. Defining resource ownership
Answer: B (LEAVE A REPLY)
Explanation
The greatest benefit of information asset classification is providing a basis for imple-menting a need-to-know policy. Information asset classification is a process of catego-rizing information based on its level of sensitivity and importance, and applying appro-priate security controls based on the level of risk associated with that information1. A need-to-know policy is a principle that states that access to information should be granted only to those individuals who require it to perform their official duties or tasks2. The purpose of a need-to-know policy is to limit the exposure of sensitive information to unauthorized or unnecessary parties, and to reduce the risk of data breaches, leaks, or misuse. Information asset classification provides a basis for implementing a need-to-know policy by:
*Defining the value and protection requirements of different types of information
*Labeling the information with the appropriate classification level, such as public, internal, confidential, secret, or top secret
*Establishing the roles and responsibilities of information owners, custodians, and users
*Enforcing access controls and encryption for the information
*Documenting the security policies and procedures for the information
By providing a basis for implementing a need-to-know policy, information asset classi-fication can help organizations to protect their sensitive information, comply with rele-vant laws and regulations, and achieve their business objectives. The other options are not the greatest benefits of information asset classification. Helping to determine the recovery point objective (RPO) is not a benefit, but rather a consequence of applying security controls based on the classification level. RPO is the acceptable amount of data loss in case of a disruption3. Supporting segregation of duties is not a benefit, but rather a prerequisite for implementing a

need-to-know policy. Segregation of duties is a principle that states that no single individual should have control over two or more phases of a business process or transaction that are susceptible to errors or fraud4. De-fining resource ownership is not a benefit, but rather a component of information asset classification. Resource ownership is the assignment of accountability and authority for an information asset to an individual or a group5. References: 1: Information Classifi-cation - Advisera 2: Need-to-Know Principle - NIST 3: Recovery Point Objective - NIST 4: Segregation of Duties - NIST 5: Resource Ownership - NIST : Information Classification in Information Security - GeeksforGeeks : Information Asset Classification Policy - UCI

NEW QUESTION: 194
A newly appointed information security manager has been asked to update all security-related policies and procedures that have been static for five years or more. What should be done NEXT?
A. Update in accordance with the best business practices.
B. Perform a risk assessment of the current IT environment.
C. Gain an understanding of the current business direction.
D. Inventory and review current security policies.
Answer: (SHOW ANSWER)
Explanation
The next step for the information security manager should be to inventory and review the current security policies to understand the existing security requirements, controls, and gaps. This will help to identify the areas that need to be updated, revised, or replaced to align with the current business needs and objectives, as well as the legal and regulatory requirements. Updating the policies in accordance with the best business practices, performing a risk assessment of the current IT environment, or gaining an understanding of the current business direction are important activities, but they should be done after reviewing the current security policies. References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Information Security Policies, Standards, Procedures and Guidelines, Subsection: Information Security Policies, Page 28.

NEW QUESTION: 195
Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of confidentiality?
A. Ensuring hashing of administrator credentials
B. Enforcing service level agreements (SLAs)
C. Ensuring encryption for data in transit
D. Utilizing a formal change management process
Answer: (SHOW ANSWER)
Explanation
Ensuring encryption for data in transit is the best activity that supports the concept of confidentiality within the CIA triad, as it protects the data from unauthorized access or interception while it is being transmitted over a network. Encryption is a technique that transforms data into an unreadable form using a secret key, so that

only authorized parties who have the key can decrypt and access the data. Encryption standards include AES (Advanced Encryption Standard) and DES (Data Encryption Standard).
References = CISM Review Manual 2022, page 321; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.12; The CIA triad: Definition, components and examples3; CIA Triad - GeeksforGeeks4

NEW QUESTION: 196
Which of the following is MOST important to ensure when developing escalation procedures for an incident response plan?
A. Each process is assigned to a responsible party.
B. The contact list is regularly updated.
C. Minimum regulatory requirements are maintained.
D. Senior management approval has been documented.
Answer: (SHOW ANSWER)
Explanation
= The contact list is the most important element of the escalation procedures for an incident response plan, as it ensures that the appropriate stakeholders are notified and involved in the incident management process. A contact list should include the names, roles, responsibilities, phone numbers, email addresses, and backup contacts of the key personnel involved in the incident response, such as the incident response team, senior management, legal counsel, public relations, law enforcement, and external service providers. The contact list should be regularly updated and tested to ensure its accuracy and availability123. References =
1: Information Security Incident Response Escalation Guideline2, page 4
2: A Practical Approach to Incident Management Escalation1, section "Step 2: Log the escalation and record the related incident problems that occurred"
3: Computer Security Incident Handling Guide4, page 18

NEW QUESTION: 197
Which of the following is MOST important to include in a report to key stakeholders regarding the effectiveness of an information security program?
A. Security metrics
B. Security baselines
C. Security incident details
D. Security risk exposure
Answer: (SHOW ANSWER)

Explanation
Security metrics are the most important to include in a report to key stakeholders regarding the effectiveness of an information security program because they provide objective and measurable evidence of security performance and progress. Security metrics can include measures such as the number and severity of security incidents, the level of compliance with security policies and standards, the effectiveness of security controls, and the return on investment (ROI) of security initiatives. The other choices may also be included in a security report, but security metrics are the most important.
An information security program is a set of policies, procedures, standards, guidelines, and tools that aim to protect an organization's information assets from threats and ensure compliance with laws and regulations. The effectiveness of an information security program depends on various factors, such as the organization's risk appetite, business objectives, resources, culture, and external environment. Regular reporting to key stakeholders, such as senior management, the board of directors, and business partners, is critical to maintaining their support and buy-in for the program. The report should provide clear and concise information on the program's status, achievements, challenges, and future plans, and it should be tailored to the audience's needs and expectations.

NEW QUESTION: 198
The PRIMARY reason to create and externally store the disk hash value when performing forensic data acquisition from a hard disk is to:
A. validate the confidentiality during analysis.
B. reinstate original data when accidental changes occur.
C. validate the integrity during analysis.
D. provide backup in case of media failure.
Answer: (SHOW ANSWER)
Explanation
The disk hash value is a unique identifier that is calculated from the binary data of the disk. It is used to verify that the disk image is an exact copy of the original disk and that no changes have occurred during the acquisition or analysis process. The disk hash value is stored externally, such as on a CD-ROM or a USB drive, to prevent tampering or corruption. The disk hash value can also be used as evidence in court to prove the authenticity and reliability of the digital evidence123 References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 2532: Guide to Computer Forensics and Investigations Fourth Edition, page 4-103: Forensic disk acquisition over the network, Andrea Fortuna, 2018.The main purpose of creating and storing an external disk hash value when performing forensic data acquisition from a hard disk is to validate the integrity of the data during the analysis. This is done by comparing the original hash value of the disk to the hash value created during the acquisition process, which can be used to ensure that the data has not been tampered with or corrupted in any way. Additionally, by creating a hash value of the disk, it can be used to quickly verify the integrity of any data that is accessed from the disk in the future.

NEW QUESTION: 199
An information security manager has recently been notified of potential security risks associated with a third-party service provider. What should be done NEXT to address this concern?

A. Escalate to the chief risk officer (CRO).
B. Conduct a vulnerability analysis.
C. Conduct a risk analysis.
D. Determine compensating controls.
Answer: (SHOW ANSWER)
Explanation
A risk analysis is the next step to identify and evaluate the potential security risks associated with a third-party service provider and determine the appropriate risk response strategies. References = CISM Review Manual, 16th Edition, Domain 2: Information Risk Management, Chapter 2: Risk Identification, p. 97-981; Chapter 3: Risk Assessment, p. 109-1101; Chapter 4: Risk Response, p. 123-1241

NEW QUESTION: 200
Which of the following should be done FIRST when a SIEM flags a potential event?
A. Validate the event is not a false positive.
B. Initiate the incident response plan.
C. Escalate the event to the business owner.
D. Implement compensating controls.
Answer: (SHOW ANSWER)
Explanation
The first thing that should be done when a SIEM flags a potential event is A. Validate the event is not a false positive. This is because a false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. False positives can waste the time and resources of the security team, and reduce the trust and confidence in the SIEM system. Therefore, it is important to verify the accuracy and validity of the event before initiating any further actions, such as incident response, escalation, or compensating controls. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise.
A false positive is an event that is incorrectly identified as malicious or suspicious by the SIEM, when in fact it is benign or normal. Validation can be done by analyzing the event data, comparing it with the baseline or normal behavior, and checking for any anomalies or indicators of compromise. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 72, page 19

NEW QUESTION: 201
Which of the following is the BEST approach to incident response for an organization migrating to a cloud-based solution?
A. Adopt the cloud provider's incident response procedures.
B. Transfer responsibility for incident response to the cloud provider.
C. Continue using the existing incident response procedures.
D. Revise incident response procedures to encompass the cloud environment.
Answer: (SHOW ANSWER)
Explanation

The best approach to incident response for an organization migrating to a cloud-based solution is to revise the existing incident response procedures to encompass the cloud environment. This is because the cloud environment introduces new challenges and risks that may not be adequately addressed by the current procedures. For example, the cloud provider may have different roles and responsibilities, service level agreements, notification and escalation processes, data protection and privacy requirements, and legal and regulatory obligations than the organization. Therefore, the organization should review and update its incident response procedures to align with the cloud provider's policies and practices, as well as the organization's business objectives and risk appetite. The organization should also ensure that the incident response team members are trained and aware of the changes in the procedures and the cloud environment.
The other options are not the best approaches because they do not consider the specific characteristics and implications of the cloud environment. Adopting the cloud provider's incident response procedures may not be feasible or desirable, as the organization may have different needs and expectations than the cloud provider. Transferring responsibility for incident response to the cloud provider may not be possible or advisable, as the organization may still retain some accountability and liability for the security and availability of its data and services in the cloud. Continuing to use the existing incident response procedures may not be effective or efficient, as the procedures may not cover the scenarios and issues that may arise in the cloud environment.
References = CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-192, 195-196, 199-200.
Cloud Incident Response Framework - A Quick Guide 2, pages 3-4, 6-7, 9-10.
CISM ITEM DEVELOPMENT GUIDE 3, page 18, Question 1.

NEW QUESTION: 202
An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk?
A. Requirement for regular information security awareness
B. Right-to-audit clause
C. Service level agreement (SLA)
D. Requirement to comply with corporate security policy
Answer: (SHOW ANSWER)
Explanation
The most effective way to mitigate information security risk when outsourcing network management to a service provider is to include a requirement for the service provider to comply with the corporate security policy in the contract. This requirement ensures that the service provider follows the same security standards, procedures, and controls as the organization, and protects the confidentiality, integrity, and availability of the organization's data and systems. The requirement also defines the roles and responsibilities, the reporting and escalation mechanisms, and the penalties for non-compliance.
References = A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance, CISM Domain 2: Information Risk Management (IRM) [2022 update]

NEW QUESTION: 203

Which of the following is the BEST method for determining whether a firewall has been configured to provide a comprehensive perimeter defense9

A. A validation of the current firewall rule set

B. A port scan of the firewall from an internal source

C. A ping test from an external source

D. A simulated denial of service (DoS) attack against the firewall

Answer: A (LEAVE A REPLY)

Explanation

A validation of the current firewall rule set is the best method for determining whether a firewall has been configured to provide a comprehensive perimeter defense because it verifies that the firewall rules are consistent, accurate, and effective in allowing or blocking traffic according to the security policies and standards of the organization. A port scan of the firewall from an internal source is not a good method because it does not test the firewall's behavior from an external perspective, which is more relevant for perimeter defense. A ping test from an external source is not a good method because it only tests the firewall's availability and responsiveness, not its security or functionality. A simulated denial of service (DoS) attack against the firewall is not a good method because it only tests the firewall's resilience and performance under high traffic load, not its security or functionality. References:

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information

https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/the-value-of-penetration-testing

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 204

Which of the following is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider?

A. Obtain an independent audit report.

B. Require the provider to follow stringent data classification procedures.

C. Include high penalties for security breaches in the contract.

D. Review the provider's information security policies.

Answer: (SHOW ANSWER)

Explanation

Requiring the provider to follow stringent data classification procedures is the BEST way to ensure data is not co-mingled or exposed when using a cloud service provider, because it helps to define the sensitivity and confidentiality levels of the data and the corresponding security controls and access policies that should be applied. Data classification procedures can help to prevent unauthorized access, disclosure, modification, or deletion of the data, as well as to segregate the data from other customers' data.

References =

CISM Review Manual, 16th Edition, ISACA, 2020, p. 72: "Data classification is the process of assigning a level of sensitivity to data that reflects its importance and the impact of its disclosure, alteration, or destruction."

CISM Review Manual, 16th Edition, ISACA, 2020, p. 73: "Data classification should be based on the business

requirements for confidentiality, integrity, and availability of the data, and should consider the legal, regulatory, and contractual obligations of the enterprise." Best Practices to Manage Risks in the Cloud - ISACA: "Commingling of data: A big concern many enterprises have with public cloud services is the commingling of data with that of the cloud provider's other customers.
One of your first questions should be: "How do you ensure that my data is not commingled with others?" How does the cloud provider ensure that only your team has access to your data?"

NEW QUESTION: 205
An organization plans to offer clients a new service that is subject to regulations. What should the organization do FIRST when developing a security strategy in support of this new service?
A. Determine security controls for the new service.
B. Establish a compliance program,
C. Perform a gap analysis against the current state
D. Hire new resources to support the service.
Answer: (SHOW ANSWER)
Explanation
A gap analysis is a process of comparing the current state of an organization's security posture with the desired or required state, and identifying the gaps or discrepancies that need to be addressed. A gap analysis helps to determine the current level of compliance with relevant regulations, standards, and best practices, and to prioritize the actions and resources needed to achieve the desired level of compliance1. A gap analysis should be performed first when developing a security strategy in support of a new service that is subject to regulations, because it provides the following benefits2:
It helps to understand the scope and impact of the new service on the organization's security objectives, risks, and controls.
It helps to identify the legal, regulatory, and contractual requirements that apply to the new service, and the potential penalties or consequences of non-compliance.
It helps to assess the effectiveness and efficiency of the existing security controls, and to identify the gaps or weaknesses that need to be remediated or enhanced.
It helps to align the security strategy with the business goals and objectives of the new service, and to ensure the security strategy is consistent and coherent across the organization.
It helps to communicate the security requirements and expectations to the stakeholders involved in the new service, and to obtain their support and commitment.
The other options, such as determining security controls for the new service, establishing a compliance program, or hiring new resources to support the service, are not the first steps when developing a security strategy in support of a new service that is subject to regulations, because they depend on the results and recommendations of the gap analysis. Determining security controls for the new service requires a clear understanding of the security requirements and risks associated with the new service, which can be obtained from the gap analysis. Establishing a compliance program requires a systematic and structured approach to implement, monitor, and improve the security controls and processes that ensure compliance, which can be based on the gap analysis. Hiring new resources to support the service requires a realistic and justified estimation of the human and financial resources needed to achieve the security objectives and compliance,

which can be derived from the gap analysis. References = 1: What is a Gap Analysis? | Smartsheet 2: CISM Review Manual 15th Edition, page 121 : CISM Review Manual 15th Edition, page 122 : CISM Review Manual 15th Edition, page 123 : CISM Review Manual 15th Edition, page 124 : CISM Review Manual 15th Edition, page 125 Learn more:
1. infosectrain.com2. resources.infosecinstitute.com3. resources.infosecinstitute.com4. resources.infosecinstitute.com+2 more

NEW QUESTION: 206
Which of the following BEST enables an organization to maintain legally admissible evidence7
A. Documented processes around forensic records retention
B. Robust legal framework with notes of legal actions
C. Chain of custody forms with points of contact
D. Forensic personnel training that includes technical actions
Answer: (SHOW ANSWER)
Explanation
Chain of custody forms with points of contact are the best way to enable an organization to maintain legally admissible evidence because they document the sequence of control, transfer, and analysis of the evidence, and every person who handled it, the dates and times, and the purpose for each action1. They also ensure the authenticity and integrity of the evidence, and prevent tampering or loss1. Documented processes around forensic records retention are not sufficient to maintain legally admissible evidence because they do not track or verify the handling of the evidence. Robust legal framework with notes of legal actions are not sufficient to maintain legally admissible evidence because they do not record or validate the preservation of the evidence. Forensic personnel training that includes technical actions are not sufficient to maintain legally admissible evidence because they do not account or certify the custody of the evidence. References: 1 https://www.researchgate.net/publication/326079761_Digital_Chain_of_Custody

NEW QUESTION: 207
Which of the following should be the FIRST step in patch management procedures when receiving an emergency security patch?
A. Schedule patching based on the criticality.
B. Install the patch immediately to eliminate the vulnerability.
C. Conduct comprehensive testing of the patch.
D. Validate the authenticity of the patch.
Answer: (SHOW ANSWER)
Explanation
Validating the authenticity of the patch is the first step in patch management procedures when receiving an emergency security patch, as it helps to ensure that the patch is genuine and not malicious. Validating the authenticity of the patch can be done by verifying the source, signature, checksum, or certificate of the patch, and comparing it with the information provided by the software vendor or manufacturer. Installing an unverified patch may introduce malware, compromise the system, or cause unexpected errors or conflicts.

References = CISM Review Manual 2022, page 3131; CISM Exam Content Outline, Domain 4, Task 4.42; Practical Patch Management and Mitigation1; Vulnerability and patch management in the CISSP exam3

NEW QUESTION: 208
Which of the following BEST enables an organization to operate smoothly with reduced capacities when service has been disrupted?
A. Crisis management plan
B. Disaster recovery plan (DRP)
C. Incident response plan
D. Business continuity plan (BCP)
Answer: (SHOW ANSWER)
Explanation
A business continuity plan (BCP) is the best option that enables an organization to operate smoothly with reduced capacities when service has been disrupted, as it defines the processes and procedures to maintain or resume critical business functions and minimize the impact of the disruption on the organization's objectives, customers, and stakeholders. A BCP also includes strategies for resource management, communication, recovery, and testing.
References = CISM Review Manual 2022, page 3101; CISM Exam Content Outline, Domain 4, Knowledge Statement 4.82; CISM 2020: Business Continuity3; Part Two: Business Continuity and Disaster Recovery Plans4

NEW QUESTION: 209
When developing an information security strategy for an organization, which of the following is MOST helpful for understanding where to focus efforts?
A. Gap analysis
B. Project plans
C. Vulnerability assessment
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
Explanation
Gap analysis is the MOST helpful tool for understanding where to focus efforts when developing an information security strategy for an organization, because it helps to identify the current state and the desired state of the information security governance, and the gaps between them. Gap analysis also helps to prioritize the actions and resources needed to close the gaps and achieve the information security objectives.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Gap analysis is the process of comparing the current state and the desired state of information security governance and identifying the gaps that need to be addressed." CISM Review Manual, 16th Edition, ISACA, 2020, p. 37: "Gap analysis should be performed periodically to assess the effectiveness and efficiency of the information security strategy and program and to identify the areas for improvement." CISM domain 1: Information security governance [Updated 2022] - Infosec

Resources: "Gap analysis: This is a comparison of the current state of security with the desired state. It helps to identify the gaps in security and prioritize the actions required to close them."

NEW QUESTION: 210

Which of the following is the BEST way to obtain support for a new organization-wide information security program?

A. Benchmark against similar industry organizations

B. Deliver an information security awareness campaign.

C. Publish an information security RACI chart.

D. Establish an information security strategy committee.

Answer: (SHOW ANSWER)

Explanation

= Establishing an information security strategy committee is the best way to obtain support for a new organization-wide information security program because it involves the participation and collaboration of key stakeholders from different business functions and levels who can provide input, guidance, and endorsement for the security program. An information security strategy committee is a governance body that oversees the development, implementation, and maintenance of the security program and aligns it with the organization's strategic objectives, risk appetite, and culture. An information security strategy committee can help to obtain support for the security program by:

Communicating the vision, mission, and goals of the security program to the organization and demonstrating its value and benefits.

Establishing roles and responsibilities for the security program and ensuring accountability and ownership.

Securing adequate resources and budget for the security program and allocating them appropriately.

Resolving conflicts and issues that may arise during the security program execution and ensuring alignment with other business processes and initiatives.

Monitoring and evaluating the performance and effectiveness of the security program and ensuring continuous improvement and adaptation.

Benchmarking against similar industry organizations is a useful technique to compare and improve the security program, but it is not the best way to obtain support for a new organization-wide information security program. Benchmarking involves measuring and analyzing the security program's processes, practices, and outcomes against those of other organizations that have similar characteristics, objectives, or challenges.

Benchmarking can help to identify gaps, strengths, weaknesses, opportunities, and threats in the security program and to adopt best practices and standards that can enhance the security program's performance and maturity. However, benchmarking alone does not guarantee the support or acceptance of the security program by the organization, as it may not reflect the organization's specific needs, risks, or culture.

Delivering an information security awareness campaign is a vital component of the security program, but it is not the best way to obtain support for a new organization-wide information security program. An information security awareness campaign is a set of activities and initiatives that aim to educate and inform the organization's workforce and other relevant parties about the security program's policies, standards, procedures, and guidelines, as well as the security risks, threats, and incidents that may affect the organization.

An information security awareness campaign can help to increase the security knowledge, skills, and behaviors of the organization's members and to foster a security risk-aware culture. However, an information security awareness campaign is not sufficient to obtain support for the security program, as it may not address the strategic, operational, or financial aspects of the security program or the expectations and interests of the different stakeholders.
Publishing an information security RACI chart is a helpful tool to define and communicate the security program's roles and responsibilities, but it is not the best way to obtain support for a new organization-wide information security program. A RACI chart is a matrix that assigns the level of involvement and accountability for each task or activity in the security program to each role or stakeholder. RACI stands for Responsible, Accountable, Consulted, and Informed, which are the four possible levels of participation. A RACI chart can help to clarify the expectations, obligations, and authority of each role or stakeholder in the security program and to avoid duplication, confusion, or conflict. However, a RACI chart does not ensure the support or commitment of the roles or stakeholders for the security program, as it may not address the benefits, challenges, or resources of the security program or the feedback and input of the roles or stakeholders.
References = CISM Review Manual 15th Edition, pages 97-98, 103-104, 107-108, 111-112 Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition - ISACA1 Information Security Strategy: The Key to Success - ISACA2 Deliver an information security awareness campaign is the BEST approach to obtain support for a new organization-wide information security program.
An information security awareness campaign is a great way to raise awareness of the importance of information security and the impact it can have on an organization. It helps to ensure that all stakeholders understand the importance of information security and are aware of the risks associated with it. Additionally, an effective awareness campaign can help to ensure that everyone in the organization is aware of the cybersecurity policies, procedures, and best practices that must be followed.

NEW QUESTION: 211
The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:
A. the internal audit manager.
B. the information security officer.
C. the steering committee.
D. the board of directors.
Answer: (SHOW ANSWER)
Explanation
The board of directors is the ultimate authority and accountability for ensuring the objectives of an information security framework are being met, as they are responsible for setting the strategic direction, approving the policies, overseeing the performance, and ensuring the compliance of the organization. The board of directors also delegates the authority and resources to the information security officer, the steering committee, and the internal audit manager, who are involved in the design, implementation, monitoring, and improvement of the information security framework.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12; CISM domain 1: Information security governance Updated 2022

NEW QUESTION: 212
An email digital signature will:
A. protect the confidentiality of an email message.
B. verify to recipient the integrity of an email message.
C. automatically correct unauthorized modification of an email message.
D. prevent unauthorized modification of an email message.
Answer: (SHOW ANSWER)
Explanation
An email digital signature will verify to recipient the integrity of an email message because it ensures that the message has not been altered or tampered with during transit, and confirms that the message originated from the sender and not an imposter. An email digital signature will not protect the confidentiality of an email message because it does not encrypt or hide the message content from unauthorized parties. An email digital signature will not automatically correct unauthorized modification of an email message because it does not change or restore the message content if it has been altered or tampered with. An email digital signature will not prevent unauthorized modification of an email message because it does not block or stop any attempts to alter or tamper with the message content. References:
https://support.microsoft.com/en-us/office/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85
https://www.techtarget.com/searchsecurity/definition/digital-signature

NEW QUESTION: 213
Which is following should be an information security manager's PRIMARY focus during the development of a critical system storing highly confidential data?
A. Reducing the number of vulnerabilities detected
B. Ensuring the amount of residual risk is acceptable
C. Avoiding identified system threats
D. Complying with regulatory requirements
Answer: B (LEAVE A REPLY)
Explanation
The information security manager's primary focus during the development of a critical system storing highly confidential data should be ensuring the amount of residual risk is acceptable. Residual risk is the level of cyber risk remaining after all the security controls are accounted for, any threats have been addressed and the

organization is meeting security standards. It's the risk that slips through the cracks of the system. For a critical system storing highly confidential data, the residual risk should be as low as possible, and within the organization's risk appetite and tolerance. The information security manager should monitor and review the residual risk throughout the system development life cycle, and ensure that it is communicated and approved by the appropriate stakeholders. The other options are not the primary focus, although they may be part of the security objectives and activities. Reducing the number of vulnerabilities detected is a desirable outcome, but it does not necessarily mean that the residual risk is acceptable, as some vulnerabilities may have a higher impact or likelihood than others. Avoiding identified system threats is a preventive measure, but it does not account for unknown or emerging threats that may pose a residual risk to the system. Complying with regulatory requirements is a mandatory obligation, but it does not guarantee that the residual risk is acceptable, as regulations may not cover all aspects of security or reflect the specific context and needs of the organization.

NEW QUESTION: 214
Which of the following is the PRIMARY objective of a business impact analysis (BIA)?
A. Determine recovery priorities.
B. Define the recovery point objective (RPO).
C. Confirm control effectiveness.
D. Analyze vulnerabilities.
Answer: (SHOW ANSWER)
Explanation
The primary objective of a business impact analysis (BIA) is to determine recovery priorities. The BIA is used to identify and analyze the potential effects of an incident on the organization, including the financial impact, operational impact, and reputational impact. The BIA also helps to identify critical resources and processes, determine recovery objectives and strategies, and develop recovery plans. Reference: Certified Information Security Manager (CISM) Study Manual, Chapter 4, Business Impact Analysis.

NEW QUESTION: 215
Which of the following will BEST enable an effective information asset classification process?
A. Including security requirements in the classification process
B. Analyzing audit findings
C. Reviewing the recovery time objective (RTO) requirements of the asset
D. Assigning ownership
Answer: (SHOW ANSWER)
Explanation
Assigning ownership is the best way to enable an effective information asset classification process, as it establishes the authority and responsibility for the information asset and its protection. The owner of the information asset should be involved in the classification process, as they have the best knowledge of the value, sensitivity, and criticality of the asset, as well as the impact of its loss or compromise. The owner should also ensure that the asset is properly labeled, handled, and secured according to its classification level.
(From CISM Review Manual 15th Edition)

References: CISM Review Manual 15th Edition, page 64, section 2.2.1.2; Information Asset and Security Classification Procedure1, section 3.1.

NEW QUESTION: 216
Which of the following is the PRIMARY purpose of an acceptable use policy?
A. To provide steps for carrying out security-related procedures
B. To facilitate enforcement of security process workflows
C. To protect the organization from misuse of information assets
D. To provide minimum security baselines for information assets
Answer: (SHOW ANSWER)
Explanation
The PRIMARY purpose of an acceptable use policy is to protect the organization from misuse of information assets, such as data, hardware, software, and network resources, by defining the rules and expectations for the authorized and appropriate use of these assets by the users. An acceptable use policy helps to prevent or reduce the risks of security breaches, legal liabilities, reputational damage, or loss of productivity that may result from unauthorized, inappropriate, or unethical use of information assets.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 74: "An acceptable use policy is a policy that establishes an agreement between users and the enterprise that defines, for all parties, the ranges of use that are approved before gaining access to a network or the Internet." The essentials of an acceptable use policy - Infosec Resources: "An Acceptable Use Policy (henceforward mentioned as "AUP") is agreement between two or more parties to a computer network community, expressing in writing their intent to adhere to certain standards of behaviour with respect to the proper usage of specific hardware & software services." Acceptable use policy template - Workable: "This Acceptable Use Policy sets the minimum requirements for the use of our company's IT resources, including computers, networks, devices, software, and internet. It aims to protect our company and our employees from harm and liability, and to ensure that our IT resources are used appropriately, productively, and securely."

NEW QUESTION: 217
Which of the following is the PRIMARY reason to perform regular reviews of the cybersecurity threat landscape?
A. To compare emerging trends with the existing organizational security posture
B. To communicate worst-case scenarios to senior management
C. To train information security professionals to mitigate new threats
D. To determine opportunities for expanding organizational information security
Answer: (SHOW ANSWER)
Explanation
The primary reason to perform regular reviews of the cybersecurity threat landscape is to compare emerging trends with the existing organizational security posture, as this helps the information security manager to identify and prioritize the gaps and risks that need to be addressed. The cybersecurity threat landscape is dynamic and constantly evolving, and the organization's security posture may not be adequate or aligned with

the current and future threats. By reviewing the threat landscape regularly, the information security manager can assess the effectiveness and maturity of the security program, and recommend appropriate actions and controls to improve the security posture and reduce the likelihood and impact of cyberattacks. References = CISM Review Manual 2023, page 831; CISM Review Questions, Answers & Explanations Manual 2023, page 322; ISACA CISM - iSecPrep, page 173

NEW QUESTION: 218
Which of the following is BEST used to determine the maturity of an information security program?
A. Security budget allocation
B. Organizational risk appetite
C. Risk assessment results
D. Security metrics
Answer: D (LEAVE A REPLY)
Explanation
Security metrics are the best way to determine the maturity of an information security program because they are quantifiable indicators of the performance and effectiveness of the security controls and processes. Security metrics help to evaluate the current state of security, identify gaps and weaknesses, measure progress and improvement, and communicate the value and impact of security to stakeholders. Therefore, security metrics are the correct answer.
References:
* https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-secur
* https://www.gartner.com/en/publications/protect-your-business-assets-with-roadmap-for-maturing-informa

NEW QUESTION: 219
Which of the following is MOST helpful for aligning security operations with the IT governance framework?
A. Security risk assessment
B. Security operations program
C. Information security policy
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
Explanation
An information security policy is the MOST helpful for aligning security operations with the IT governance framework because it defines the security objectives, principles, standards, and guidelines that guide the security operations activities and processes. An information security policy also establishes the roles and responsibilities, authorities and accountabilities, and reporting and communication mechanisms for security operations. An information security policy should be aligned with the IT governance framework, which provides the direction, structure, and oversight for the effective management and delivery of IT services and resources. An information security policy should also be consistent with the enterprise governance framework, which sets the vision, mission, values, and goals of the organization12. A security risk assessment (A) is helpful for identifying and evaluating the security risks that may affect the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A security risk assessment should be based on the

information security policy, which defines the risk appetite, tolerance, and criteria for the organization12. A security operations program (B) is helpful for implementing and executing the security operations activities and processes that support the IT governance framework, but it is not the MOST helpful for aligning them. A security operations program should be derived from the information security policy, which provides the strategic direction and guidance for the security operations12. A business impact analysis (BIA) (D) is helpful for determining the criticality and priority of the business processes and functions that depend on the security operations and the IT governance framework, but it is not the MOST helpful for aligning them. A BIA should be conducted in accordance with the information security policy, which specifies the business continuity and disaster recovery requirements and objectives for the organization12. References = 1: CISM Review Manual 15th Edition, page 75-76, 81-82, 88-89, 93-941; 2:
CISM Domain 1: Information Security Governance (ISG) [2022 update]2

NEW QUESTION: 220

Embedding security responsibilities into job descriptions is important PRIMARILY because it:

A. supports access management.
B. simplifies development of the security awareness program.
C. aligns security to the human resources (HR) function.
D. strengthens employee accountability.
Answer: D (LEAVE A REPLY)
Explanation
Comprehensive and Detailed Explanation: Employee accountability is the degree to which employees are responsible for their actions and outcomes related to information security. It reflects the extent to which employees understand their roles and responsibilities, follow the policies and procedures, report incidents and breaches, and comply with legal and regulatory requirements. Embedding security responsibilities into job descriptions helps to clarify the expectations and obligations of employees, as well as the consequences of non-compliance or negligence. It also helps to align the security objectives with the business goals and strategies, and to foster a culture of security awareness and responsibility.
References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.2

NEW QUESTION: 221
The PRIMARY objective of performing a post-incident review is to:
A. re-evaluate the impact of incidents.
B. identify vulnerabilities.
C. identify control improvements.
D. identify the root cause.
Answer: (SHOW ANSWER)
Explanation
= The primary objective of performing a post-incident review is to identify the root cause of the incident, which is the underlying factor or condition that enabled or facilitated the occurrence of the incident.
Identifying the root cause helps to understand the nature and origin of the incident, and to prevent or mitigate similar incidents in the future. A post-incident review also aims to evaluate the effectiveness and efficiency of

the incident response process, identify lessons learned and best practices, and recommend improvements for the incident management policies, procedures, controls, and tools. However, these are secondary objectives that depend on the identification of the root cause as the first step.
Re-evaluating the impact of incidents is not the primary objective of performing a post-incident review, as it is already done during the incident response process. The impact of incidents is the extent and severity of the damage or harm caused by the incident to the organization's assets, operations, reputation, or stakeholders. Re-evaluating the impact of incidents may be part of the post-incident review, but it is not the main goal.
Identifying vulnerabilities is not the primary objective of performing a post-incident review, as it is also done during the incident response process. Vulnerabilities are weaknesses or flaws in the system or network that can be exploited by attackers to compromise the confidentiality, integrity, or availability of the information or resources. Identifying vulnerabilities may be part of the post-incident review, but it is not the main goal.
Identifying control improvements is not the primary objective of performing a post-incident review, as it is a result of the root cause analysis. Controls are measures or mechanisms that are implemented to protect the system or network from threats, reduce risks, or ensure compliance with policies and standards. Identifying control improvements is an important outcome of the post-incident review, but it is not the main goal.
References = ISACA CISM: PRIMARY goal of a post-incident review should be to?
CISM Exam Overview - Vinsys
CISM Review Manual, Chapter 4, page 176
CISM Exam Content Outline | CISM Certification | ISACA, Domain 4, Task 4.3

NEW QUESTION: 222
Which of the following is the PRIMARY reason to assign a risk owner in an organization?
A. To remediate residual risk
B. To define responsibilities
C. To ensure accountability
D. To identify emerging risk
Answer: (SHOW ANSWER)
Explanation
The primary reason to assign a risk owner in an organization is to ensure accountability for the risk and its treatment. A risk owner is a person or entity that has the authority and responsibility to manage a specific risk and to implement the appropriate risk response actions. By assigning a risk owner, the organization can ensure that the risk is monitored, reported, and controlled in accordance with the organization's risk appetite and tolerance.
References: The CISM Review Manual 2023 defines risk owner as "the person or entity with the accountability and authority to manage a risk" and states that "the risk owner is responsible for ensuring that the risk is treated in a manner consistent with the enterprise's risk appetite and tolerance" (p. 93). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "To ensure accountability is the correct answer because it is the primary reason to assign a risk owner in an organization, as it ensures that the risk and its treatment are managed by a person or entity that has the authority and responsibility to do so" (p. 29). Additionally, the article Risk Ownership: The First Step of Effective Risk Management from the ISACA Journal 2019 states that "risk ownership is the first and most

important step of effective risk management" and that "risk ownership ensures that there is clear accountability and responsibility for each risk and that risk owners are empowered to make risk decisions and implement risk responses" (p. 1)

NEW QUESTION: 223
Of the following, who is MOST appropriate to own the risk associated with the failure of a privileged access control?
A. Data owner
B. Business owner
C. Information security manager
D. Compliance manager
Answer: (SHOW ANSWER)
Explanation
The business owner is the most appropriate person to own the risk associated with the failure of a privileged access control because they are ultimately responsible for the protection and use of the information in their business unit1. The data owner is responsible for determining the access rights for specific data sets, but not for the access control mechanisms2. The information security manager is responsible for implementing and enforcing the security policies and standards, but not for owning the risk3. The compliance manager is responsible for ensuring that the organization meets the regulatory requirements, but not for owning the risk3.
References: 1
https://www.cyberark.com/resources/blog/how-do-you-prioritize-risk-for-privileged-access-management 3
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/capability-framework-for-privileged-access
2
https://security.stackexchange.com/questions/218049/what-is-the-difference-between-data-owner-data-custodian

NEW QUESTION: 224
An organization recently outsourced the development of a mission-critical business application. Which of the following would be the BEST way to test for the existence of backdoors?
A. Scan the entire application using a vulnerability scanning tool.
B. Run the application from a high-privileged account on a test system.
C. Perform security code reviews on the entire application.
D. Monitor Internet traffic for sensitive information leakage.
Answer: (SHOW ANSWER)
Explanation
The best way to test for the existence of backdoors in a mission-critical business application that was outsourced to a third-party developer is to perform security code reviews on the entire application. A backdoor is a hidden or undocumented feature or function in a software application that allows unauthorized or remote access, control, or manipulation of the application or the system it runs on. Backdoors can be intentionally or unintentionally introduced by the developers, or maliciously inserted by the attackers, and they can pose

serious security risks and threats to the organization and its data. Security code reviews are the process of examining and analyzing the source code of a software application to identify and eliminate any security vulnerabilities, flaws, or weaknesses, such as backdoors, that may compromise the functionality, performance, or integrity of the application or the system. Security code reviews can be performed manually by the security experts, or automatically by the security tools, or both, and they can be done at different stages of the software development life cycle, such as design, coding, testing, or deployment. Security code reviews can help to detect and remove any backdoors in the application before they can be exploited by the attackers, and they can also help to improve the quality, reliability, and security of the application.
References = CISM Review Manual, 16th Edition, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Development, page 1581; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 87, page 812; CISM ITEM DEVELOPMENT GUIDE, page 63.

NEW QUESTION: 225
Which of the following would be MOST effective in reducing the impact of a distributed denial of service (DDoS) attack?
A. Impose state limits on servers.
B. Spread a site across multiple ISPs.
C. Block the attack at the source.
D. Harden network security.
Answer: (SHOW ANSWER)
Explanation
The answer to the question is B. Spread a site across multiple ISPs. This is because spreading a site across multiple Internet service providers (ISPs) can help to reduce the impact of a distributed denial of service (DDoS) attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. Spreading a site across multiple ISPs can also help to distribute the traffic load and balance the performance of the site, and to mitigate the effects of regional or network-specific outages or disruptions. Spreading a site across multiple ISPs can be done by using various techniques, such as anycast routing, content delivery networks (CDNs), or cloud-based services12.
Spreading a site across multiple ISPs can help to reduce the impact of a DDoS attack by increasing the bandwidth and redundancy of the site, and making it harder for the attacker to target and overwhelm a single point of failure. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.1, page 2091; DDoS Attacks-A Cyberthreat and Possible Solutions2

NEW QUESTION: 226
During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:
A. perform a risk assessment.
B. review the state of security awareness.
C. review information security policies.
D. perform a gap analysis.

Answer: (SHOW ANSWER)

Explanation

According to the CISM Review Manual, performing a risk assessment is the most important course of action for an information security manager during the due diligence phase of an acquisition, as it helps to identify and evaluate the potential threats, vulnerabilities and impacts that may affect the information assets of the target organization. A risk assessment also provides the basis for performing a gap analysis, reviewing the information security policies and awareness, and developing a remediation plan.

References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.4.1, page 1411.

NEW QUESTION: 227

An organization has purchased an Internet sales company to extend the sales department. The information security manager's FIRST step to ensure the security policy framework encompasses the new business model is to:

A. perform a gap analysis.

B. implement both companies' policies separately

C. merge both companies' policies

D. perform a vulnerability assessment

Answer: (SHOW ANSWER)

Explanation

Performing a gap analysis is the first step to ensure the security policy framework encompasses the new business model because it is a process of comparing the current state of security policies and controls with the desired or required state. A gap analysis helps to identify the strengths and weaknesses of the existing security policy framework, as well as the opportunities and threats posed by the new business model. A gap analysis also helps to prioritize the actions and resources needed to close the gaps and align the security policy framework with the new business objectives and requirements. Therefore, performing a gap analysis is the correct answer.

References:

https://secureframe.com/blog/security-frameworks

https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-o

NEW QUESTION: 228

A penetration test against an organization's external web application shows several vulnerabilities. Which of the following presents the GREATEST concern?

A. A rules of engagement form was not signed prior to the penetration test
B. Vulnerabilities were not found by internal tests
C. Vulnerabilities were caused by insufficient user acceptance testing (UAT)
D. Exploit code for one of the vulnerabilities is publicly available
Answer: (SHOW ANSWER)
Explanation
Exploit code for one of the vulnerabilities is publicly available presents the greatest concern because it means that anyone can easily exploit the vulnerability and compromise the web application. This increases the risk of data breach, denial of service, or other malicious attacks. Therefore, exploit code for one of the vulnerabilities is publicly available is the correct answer.
References:
* https://www.imperva.com/learn/application-security/penetration-testing/
* https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your-web-appl

NEW QUESTION: 229
When determining an acceptable risk level which of the following is the MOST important consideration?
A. Threat profiles
B. System criticalities
C. Vulnerability scores
D. Risk matrices
Answer: (SHOW ANSWER)
Explanation
The effectiveness of an incident response team will be greatest when the incident response process is updated based on lessons learned. This ensures that the team can continuously improve its performance and capabilities, and address any gaps or weaknesses identified during previous incidents. Updating the incident response process based on lessons learned also helps to align the process with the changing business and security environment, and to incorporate best practices and standards. Meeting on a regular basis to review log files, having trained security personnel as team members, and using a security information and event monitoring (SIEM) system are all important factors for an incident response team, but they are not sufficient to ensure the effectiveness of the team. Reviewing log files may help to detect and analyze incidents, but it does not guarantee that the team can respond appropriately and efficiently. Having trained security personnel may enhance the skills and knowledge of the team, but it does not ensure that the team can work collaboratively and communicate effectively. Using a SIEM system may facilitate the identification and prioritization of incidents, but it does not ensure that the team can follow the established procedures and protocols.
References = CISM Review Manual, 16th Edition, page 1361; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1492

NEW QUESTION: 230
An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

A. The information security manager

B. The data custodian
C. Internal IT audit
D. The data owner
Answer: (SHOW ANSWER)
Explanation
The data custodian is the person or role who is responsible for enforcing authorized and controlled access to the CRM data, according to the security policies and standards defined by the data owner. The data custodian implements and maintains the technical and operational controls, such as authentication, authorization, encryption, backup, and recovery, to protect the data from unauthorized access, modification, disclosure, or destruction. The data custodian also monitors and reports on the data access activities and incidents. References = Setting Up Access Controls and Permissions in Your CRM, Accountability for Information Security Roles and Responsibilities, Part 1, How to Meet the Shared Responsibility Model with CIS

NEW QUESTION: 231
Which of the following should be an information security manager s MOST important consideration when determining the priority for implementing security controls?
A. Alignment with industry benchmarks
B. Results of business impact analyses (BIAs)
C. Possibility of reputational loss due to incidents
D. Availability of security budget
Answer: (SHOW ANSWER)
Explanation
The priority for implementing security controls should be based on the results of BIAs, which identify the criticality and recovery requirements of business processes and the supporting information assets. BIAs help to align security controls with business needs and objectives, and to optimize the allocation of security resources. Alignment with industry benchmarks, possibility of reputational loss due to incidents, and availability of security budget are important factors, but they are not the most important consideration for determining the priority for implementing security controls. References = CISM Review Manual, 16th Edition, page 971; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 2672

NEW QUESTION: 232
Which of the following will have the GREATEST influence on the successful adoption of an information security governance program?
A. Security policies
B. Control effectiveness
C. Security management processes
D. Organizational culture
Answer: (SHOW ANSWER)
Explanation
Organizational culture is the set of shared values, beliefs, and norms that influence the way employees think, feel, and behave in the workplace. It affects how employees perceive the importance of information security,

how they comply with security policies and procedures, and how they support security initiatives and goals. A strong security culture can foster a sense of ownership, responsibility, and accountability among employees, as well as a positive attitude toward security awareness and training. A weak security culture can lead to resistance, indifference, or hostility toward security efforts, as well as increased risks of human errors, negligence, or malicious actions. Therefore, organizational culture has the greatest influence on the successful adoption of an information security governance program, which requires the commitment and involvement of all levels of the organization. References = CISM Review Manual 15th Edition, page 30-31.
Learn more:

NEW QUESTION: 233
If civil litigation is a goal for an organizational response to a security incident, the PRIMARY step should be to:
A. contact law enforcement.
B. document the chain of custody.
C. capture evidence using standard server-backup utilities.
D. reboot affected machines in a secure area to search for evidence.
Answer: (SHOW ANSWER)
Explanation
Documenting the chain of custody is the PRIMARY step for an organizational response to a security incident if civil litigation is a goal because it ensures the integrity, authenticity, and admissibility of the evidence collected from the incident. The chain of custody is the process of documenting the history of the evidence, including its identification, collection, preservation, transportation, analysis, storage, and presentation in court.
The chain of custody should include information such as the date, time, location, description, source, owner, handler, and purpose of each evidence item, as well as any changes, modifications, or transfers that occurred to the evidence. Documenting the chain of custody can help to prevent the evidence from being tampered with, altered, lost, or destroyed, and to demonstrate that the evidence is relevant, reliable, and original12.
Contacting law enforcement (A) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a possible or optional step depending on the nature, severity, and jurisdiction of the incident. Contacting law enforcement may help to obtain legal assistance, guidance, or support, but it may also involve risks such as loss of control, confidentiality, or reputation. Therefore, contacting law enforcement should be done after careful consideration of the legal obligations, contractual agreements, and organizational policies12. Capturing evidence using standard server-backup utilities is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Capturing evidence using standard server-backup utilities may help to preserve the state of the systems or networks involved in the incident, but it may also introduce changes or errors that could compromise the validity or quality of the evidence. Therefore, capturing evidence using standard server-backup utilities should be done using forensically sound methods and tools, and following the documented chain of custody12. Rebooting affected machines in a secure area to search for evidence (D) is not the PRIMARY step for an organizational response to a security incident if civil litigation is a goal, but rather a technical step that should be done after documenting the chain of custody. Rebooting affected machines in a secure area may help to isolate and analyze the systems or networks involved in the incident, but it may also cause the loss or alteration of the evidence, such as volatile memory, temporary files,

or logs. Therefore, rebooting affected machines in a secure area should be done with caution and following the documented chain of custody12. References = 1: CISM Review Manual 15th Edition, page 310-3111; 2: CISM Domain 4: Information Security Incident Management (ISIM) [2022 update]2

NEW QUESTION: 234
The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:
A. results of exit interviews.
B. previous training sessions.
C. examples of help desk requests.
D. responses to security questionnaires.
Answer: (SHOW ANSWER)
Explanation
The best way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include examples of help desk requests. Help desk requests are requests for assistance or support from users who encounter problems or issues related to information security, such as password resets, malware infections, phishing emails, unauthorized access, data loss, or system errors. Help desk requests can provide valuable insights into the types, frequencies, and impacts of the incidents that affect the users, as well as the users' knowledge, skills, and behaviors regarding information security. By including examples of help desk requests in the user security awareness training program, the information security manager can achieve the following benefits12:
Increase the relevance and effectiveness of the training content: By using real-life scenarios and cases that the users have experienced or witnessed, the information security manager can make the training content more relevant, engaging, and applicable to the users' needs and situations. The information security manager can also use the examples of help desk requests to illustrate the consequences and costs of the incidents, and to highlight the best practices and solutions to prevent or resolve them. This can help the users to understand the importance and value of information security, and to improve their knowledge, skills, and attitudes accordingly.
Identify and address the gaps and weaknesses in the training program: By analyzing the patterns and trends of the help desk requests, the information security manager can identify and address the gaps and weaknesses in the existing training program, such as outdated or inaccurate information, insufficient or ineffective coverage of topics, or lack of feedback or evaluation. The information security manager can also use the examples of help desk requests to measure and monitor the impact and outcomes of the training program, such as changes in the number, type, or severity of the incidents, or changes in the users' satisfaction, performance, or behavior.
Enhance the communication and collaboration with the users and the help desk staff: By including examples of help desk requests in the user security awareness training program, the information security manager can enhance the communication and collaboration with the users and the help desk staff, who are the key stakeholders and partners in information security. The information security manager can use the examples of help desk requests to solicit feedback, suggestions, or questions from the users and the help desk staff, and to provide them with timely and relevant information, guidance, or support. The information security manager can also use the examples of help desk requests to recognize and appreciate the efforts and contributions of the

users and the help desk staff in reporting, responding, or resolving the incidents, and to encourage and motivate them to continue their involvement and participation in information security.
The other options are not the best way to ensure that frequently encountered incidents are reflected in the user security awareness training program, as they are less reliable, relevant, or effective sources of information. Results of exit interviews are feedback from employees who are leaving the organization, and they may not reflect the current or future incidents that the remaining or new employees may face. Previous training sessions are records of the past training activities, and they may not capture the changes or updates in the information security environment, threats, or requirements. Responses to security questionnaires are answers to predefined questions or surveys, and they may not cover all the possible or emerging incidents that the users may encounter or experience12. References = Information Security Awareness Training: Best Practices - Infosec Resources, How to Create an Effective Security Awareness Training Program - Infosec Resources, Security Awareness Training: How to Build a Successful Program - ISACA, Security Awareness Training: How to Educate Your Employees - ISACA

NEW QUESTION: 235
Which of the following BEST enables the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption?
A. Service level agreement (SLA)
B. Business continuity plan (BCP)
C. Disaster recovery plan (DRP)
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
Explanation
The best option to enable the capability of an organization to sustain the delivery of products and services within acceptable time frames and at predefined capacity during a disruption is B. Business continuity plan (BCP). This is because a BCP is a documented collection of procedures and information that guides the organization to prepare for, respond to, and recover from a disruption, such as a natural disaster, a cyberattack, or a pandemic. A BCP aims to ensure the continuity of the critical business functions and processes that support the delivery of products and services to the customers and stakeholders. A BCP also defines the roles, responsibilities, resources, and actions required to maintain the operational resilience of the organization in the face of a disruption.
References = CISM Review Manual 15th Edition, Chapter 4, Section 4.2.3, page 2141; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 6, page 3

NEW QUESTION: 236
A security incident has been reported within an organization. When should an inforrnation security manager contact the information owner? After the:
A. incident has been confirmed.
B. incident has been contained.
C. potential incident has been logged.
D. incident has been mitigated.

Answer: A (LEAVE A REPLY)

Explanation

= The information security manager should contact the information owner after the incident has been confirmed, as this is the first step of the incident response process. The information owner is the person who has the authority and responsibility for the information asset that is affected by the incident. The information owner needs to be informed of the incident as soon as possible, as they may have to make decisions or take actions regarding the protection, recovery, or restoration of the information asset. The information owner may also have to communicate with other stakeholders, such as the business units, customers, regulators, or media, depending on the nature and impact of the incident.

The other options are not the correct time to contact the information owner, as they occur later in the incident response process. Contacting the information owner after the incident has been contained, mitigated, or logged may delay the notification and escalation of the incident, as well as the involvement and collaboration of the information owner. Moreover, contacting the information owner after the incident has been contained or mitigated may imply that the incident response team has already taken actions that may affect the information asset without the consent or approval of the information owner. Contacting the information owner after a potential incident has been logged may cause unnecessary alarm or confusion, as the potential incident may not be a real or significant incident, or it may not affect the information owner's asset. References = CISM Review Manual, 16th Edition, ISACA, 2022, pp. 219-220, 226-227.

CISM Questions, Answers & Explanations Database, ISACA, 2022, QID 1009.

NEW QUESTION: 237

Management would like to understand the risk associated with engaging an Infrastructure-as-a-Service (IaaS) provider compared to hosting internally. Which of the following would provide the BEST method of comparing risk scenarios?

A. Mapping risk scenarios according to sensitivity of data

B. Reviewing mitigating and compensating controls for each risk scenario

C. Mapping the risk scenarios by likelihood and impact on a chart

D. Performing a risk assessment on the IaaS provider

Answer: (SHOW ANSWER)

Explanation

Mapping the risk scenarios by likelihood and impact on a chart is the best method of comparing risk scenarios, as it helps to visualize and prioritize the different types and levels of risks associated with each option. A chart can also facilitate the communication and decision-making process by showing the trade-offs and benefits of each option. A chart can be based on qualitative or quantitative data, depending on the availability and accuracy of the information.

References = CISM Review Manual 2022, page 371; CISM Exam Content Outline, Domain 1, Task 1.32; A risk assessment model for selecting cloud service providers; Security best practices for IaaS workloads in Azure

NEW QUESTION: 238

An organization implemented a number of technical and administrative controls to mitigate risk associated with ransomware. Which of the following is MOST important to present to senior management when reporting on the performance of this initiative?

A. The total cost of the investment

B. The cost and associated risk reduction

C. The number and severity of ransomware incidents

D. Benchmarks of industry peers impacted by ransomware

Answer: (SHOW ANSWER)

Explanation

The most important information to present to senior management when reporting on the performance of the initiative to mitigate risk associated with ransomware is the cost and associated risk reduction, which means showing the value and effectiveness of the technical and administrative controls in terms of reducing the likelihood and impact of ransomware incidents and data extortion, and comparing them with the investment and resources required to implement and maintain them. The cost and associated risk reduction can help senior management to evaluate the return on investment (ROI) and the alignment with the business objectives and risk appetite of the initiative.

References = Ransomware Risk Management - NIST, #StopRansomware Guide | CISA

NEW QUESTION: 239

Which of the following is the BEST way to determine the effectiveness of an incident response plan?

A. Reviewing previous audit reports

B. Conducting a tabletop exercise

C. Benchmarking the plan against best practices

D. Performing a penetration test

Answer: (SHOW ANSWER)

Explanation

A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and tests the roles, responsibilities, and procedures of the incident response plan. It is the best way to determine the effectiveness of the plan because it allows the participants to identify and address any gaps, weaknesses, or ambiguities in the plan, as well as to evaluate the communication, coordination, and decision-making processes. A tabletop exercise can also help to raise awareness, enhance skills, and improve teamwork among the incident response team members and other relevant parties.

NEW QUESTION: 240

Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?

A. Increase the frequency of system backups.

B. Review the mitigating security controls.

C. Notify staff members of the threat.

D. Assess the risk to the organization.

Answer: (SHOW ANSWER)

Explanation
The best course of action for an information security manager when a threat intelligence report indicates a large number of ransomware attacks targeting the industry is to assess the risk to the organization. This means evaluating the likelihood and impact of a potential ransomware attack on the organization's assets, operations, and reputation, based on the current threat landscape, the organization's security posture, and the effectiveness of the existing security controls. A risk assessment can help the information security manager prioritize the most critical assets and processes, identify the gaps and weaknesses in the security architecture, and determine the appropriate risk response strategies, such as avoidance, mitigation, transfer, or acceptance. A risk assessment can also provide a business case for requesting additional resources or support from senior management to improve the organization's security resilience and readiness. The other options are not the best course of action because they are either too reactive or too narrow in scope. Increasing the frequency of system backups (A) is a good practice to ensure data availability and recovery in case of a ransomware attack, but it does not address the prevention or detection of the attack, nor does it consider the potential data breach or extortion that may accompany the attack. Reviewing the mitigating security controls (B) is a part of the risk assessment process, but it is not sufficient by itself. The information security manager should also consider the threat sources, the vulnerabilities, the impact, and the risk appetite of the organization. Notifying staff members of the threat is a useful awareness and education measure, but it should be done after the risk assessment and in conjunction with other security policies and procedures. Staff members should be informed of the potential risks, the indicators of compromise, the reporting mechanisms, and the best practices to avoid or respond to a ransomware attack. References = CISM Review Manual 2022, pages 77-78, 81-82, 316; CISM Item Development Guide 2022, page 9; #StopRansomware Guide | CISA; [The Human Consequences of Ransomware Attacks - ISACA]; [Ransomware Response, Safeguards and Countermeasures - ISACA]

NEW QUESTION: 241
Which of the following metrics is MOST appropriate for evaluating the incident notification process?
A. Average total cost of downtime per reported incident
B. Elapsed time between response and resolution
C. Average number of incidents per reporting period
D. Elapsed time between detection, reporting, and response
Answer: (SHOW ANSWER)
Explanation
Elapsed time between detection, reporting, and response is the most appropriate metric for evaluating the incident notification process because it measures how quickly and effectively the organization identifies, communicates, and responds to security incidents. The incident notification process is a critical part of the incident response plan that defines the roles and responsibilities, procedures, and channels for reporting and escalating security incidents to the relevant stakeholders. Elapsed time between detection, reporting, and response helps to assess the performance and efficiency of the incident notification process, as well as to identify any bottlenecks or delays that may affect the incident resolution and recovery. Therefore, elapsed time between detection, reporting, and response is the correct answer.
References:
* https://www.atlassian.com/incident-management/kpis/common-metrics

* https://securityscorecard.com/blog/how-to-use-incident-response-metrics/
* https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

NEW QUESTION: 242
Which of the following is MOST important to ensuring information stored by an organization is protected appropriately?
A. Defining information stewardship roles
B. Defining security asset categorization
C. Assigning information asset ownership
D. Developing a records retention schedule
Answer: (SHOW ANSWER)
Explanation
The most important factor to ensuring information stored by an organization is protected appropriately is assigning information asset ownership. Information asset ownership is the process of identifying and assigning the roles and responsibilities of the individuals or groups who have the authority and accountability for the information assets and their protection. Information asset owners are responsible for defining the business value, classification, and security requirements of the information assets, as well as granting the access rights and privileges to the information users and custodians. Information asset owners are also responsible for monitoring and reviewing the security performance and compliance of the information assets, and reporting and resolving any security issues or incidents. By assigning information asset ownership, the organization can ensure that the information assets are properly identified, categorized, protected, and managed according to their importance, sensitivity, and regulatory obligations.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Data Classification, page 331; CISM Review Questions, Answers & Explanations Manual, 10th Edition, Question 62, page 572.

NEW QUESTION: 243
A KEY consideration in the use of quantitative risk analysis is that it:
A. aligns with best practice for risk analysis of information assets.
B. assigns numeric values to exposures of information assets.
C. applies commonly used labels to information assets.
D. is based on criticality analysis of information assets.
Answer: (SHOW ANSWER)

Explanation
A key consideration in the use of quantitative risk analysis is that it assigns numeric values to exposures of information assets, such as the probability of occurrence, the frequency of occurrence, the impact of occurrence, and the monetary value of the assets. These numeric values help to measure and compare the risks in a more objective and consistent way, and to support the decision-making process based on cost-benefit analysis. Quantitative risk analysis also requires reliable and accurate data sources, and it may involve the use of statistical tools and techniques.
References = CISM Review Manual, 16th Edition eBook1, Chapter 2: Information Risk Management, Section: Risk Analysis, Subsection: Quantitative Risk Analysis, Page 84.

NEW QUESTION: 244
Which of the following processes BEST supports the evaluation of incident response effectiveness?
A. Root cause analysis
B. Post-incident review
C. Chain of custody
D. Incident logging
Answer: (SHOW ANSWER)
Explanation
A post-incident review (PIR) is the process of evaluating the effectiveness of the incident response after the incident has been resolved. A PIR aims to identify the strengths and weaknesses of the response process, the root causes and impacts of the incident, the lessons learned and best practices, and the recommendations and action plans for improvement1. A PIR can help an organization enhance its incident response capabilities, reduce the likelihood and severity of future incidents, and increase its resilience and maturity2.
A PIR is the best process to support the evaluation of incident response effectiveness, because it provides a systematic and comprehensive way to assess the performance and outcomes of the response process, and to identify and implement the necessary changes and improvements. A PIR involves collecting and analyzing relevant data and feedback from various sources, such as incident logs, reports, evidence, metrics, surveys, interviews, and observations. A PIR also involves comparing the actual response with the expected or planned response, and measuring the achievement of the response objectives and the satisfaction of the stakeholders3.
A PIR also involves documenting and communicating the findings, conclusions, and recommendations of the evaluation, and ensuring that they are followed up and implemented.
The other options are not as good as a PIR in supporting the evaluation of incident response effectiveness, because they are either more specific, limited, or dependent on a PIR. A root cause analysis (RCA) is a technique to identify the underlying factors or reasons that caused the incident, and to prevent or mitigate their recurrence. An RCA can help an organization understand the nature and origin of the incident, and to address the problem at its source, rather than its symptoms. However, an RCA is not sufficient to evaluate the effectiveness of the response process, because it does not cover other aspects, such as the response performance, outcomes, impacts, lessons, and best practices. An RCA is usually a part of a PIR, rather than a separate process. A chain of custody (CoC) is a process of maintaining and documenting the integrity and security of the evidence collected during the incident response. A CoC can help an organization ensure that

the evidence is reliable, authentic, and admissible in legal or regulatory proceedings. However, a CoC is not a process to evaluate the effectiveness of the response process, but rather a requirement or a standard to follow during the response process. A CoC does not provide any feedback or analysis on the response performance, outcomes, impacts, lessons, or best practices. An incident logging is a process of recording and tracking the details and activities of the incident response. An incident logging can help an organization monitor and manage the response process, and to provide an audit trail and a source of information for the evaluation. However, an incident logging is not a process to evaluate the effectiveness of the response process, but rather an input or a tool for the evaluation. An incident logging does not provide any assessment or measurement on the response performance, outcomes, impacts, lessons, or best practices. References = 1: CISM Review Manual 15th Edition, Chapter 5, Section 5.5 2: Post-Incident Review: A Guide to Effective Incident Response 3: Post-Incident Review: A Guide to Effective Incident Response : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.5 : CISM Review Manual 15th Edition, Chapter 5, Section 5.4 : CISM Review Manual 15th Edition, Chapter 5, Section 5.3

NEW QUESTION: 245
An organization wants to integrate information security into its HR management processes. Which of the following should be the FIRST step?
A. Benchmark the processes with best practice to identify gaps.
B. Calculate the return on investment (ROI).
C. Provide security awareness training to HR.
D. Assess the business objectives of the processes.
Answer: (SHOW ANSWER)

NEW QUESTION: 246
In the context of developing an information security strategy, which of the following provides the MOST useful input to determine the or
A. Security budget
B. Risk register
C. Risk score
D. Laws and regulations
Answer: (SHOW ANSWER)
Explanation
Laws and regulations provide the most useful input to determine the organization's information security strategy because they define the legal and compliance requirements and obligations that the organization must adhere to, and guide the development and implementation of the security policies and controls that support them. Security budget is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security needs or goals, but rather a resource to enable the security activities and initiatives. Risk register is not a useful input to determine the organization's information security strategy because it does not reflect the organization's security vision or mission, but rather a tool to identify and manage the security risks. Risk score is not a useful input to determine the organization's

information security strategy because it does not reflect the organization's security priorities or objectives, but rather a measure of the level of risk exposure or performance. References:
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-busin

NEW QUESTION: 247
The PRIMARY consideration when responding to a ransomware attack should be to ensure:
A. backups are available.
B. the most recent patches have been applied.
C. the ransomware attack is contained
D. the business can operate
Answer: (SHOW ANSWER)
Explanation
Ensuring the business can operate is the primary consideration when responding to a ransomware attack because it helps to minimize the disruption and impact of the attack on the organization's mission-critical functions and services. Ransomware is a type of malware that encrypts the files or systems of the victims and demands payment for their decryption. Ransomware attacks can cause significant operational, financial, and reputational damage to organizations, especially if they affect their core business processes or customer data. Therefore, ensuring the business can operate is the primary consideration when responding to a ransomware attack.
References:
https://www.cisa.gov/stopransomware/ransomware-guide
https://csrc.nist.gov/Projects/ransomware-protection-and-response
https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect-respond

NEW QUESTION: 248
An information security manager believes that information has been classified inappropriately, = the risk of a breach. Which of the following is the information security manager's BEST action?
A. Refer the issue to internal audit for a recommendation.
B. Re-classify the data and increase the security level to meet business risk.
C. Instruct the relevant system owners to reclassify the data.
D. Complete a risk assessment and refer the results to the data owners.
Answer: (SHOW ANSWER)
Explanation
= Information classification is the process of assigning appropriate labels to information assets based on their sensitivity and value to the organization. Information classification should be aligned with the business objectives and risk appetite of the organization, and should be reviewed periodically to ensure its accuracy and relevance. The information security manager is responsible for establishing and maintaining the information classification policy and procedures, as well as providing guidance and oversight to the data owners and custodians. Data owners are the individuals who have the authority and accountability for the information

assets within their business unit or function. Data owners are responsible for determining the appropriate classification level and security controls for their information assets, as well as ensuring compliance with the information classification policy and procedures. Data custodians are the individuals who have the operational responsibility for implementing and maintaining the security controls for the information assets assigned to them by the data owners.
If the information security manager believes that information has been classified inappropriately, increasing the risk of a breach, the best action is to complete a risk assessment and refer the results to the data owners. A risk assessment is a systematic process of identifying, analyzing, and evaluating the risks associated with the information assets, and recommending appropriate risk treatment options. By conducting a risk assessment, the information security manager can provide objective and evidence-based information to the data owners, highlighting the potential impact and likelihood of a breach, as well as the cost and benefit of implementing additional security controls. This will enable the data owners to make informed decisions about the appropriate classification level and security controls for their information assets, and to justify and document any deviations from the information classification policy and procedures.
The other options are not the best actions for the information security manager. Refering the issue to internal audit for a recommendation is not the best action, because internal audit is an independent and objective assurance function that provides assurance on the effectiveness of governance, risk management, and control processes. Internal audit is not responsible for providing recommendations on information classification, which is a management responsibility. Re-classifying the data and increasing the security level to meet business risk is not the best action, because the information security manager does not have the authority or accountability for the information assets, and may not have the full understanding of the business context and objectives of the data owners. Instructing the relevant system owners to reclassify the data is not the best action, because system owners are not the same as data owners, and may not have the authority or accountability for the information assets either. System owners are the individuals who have the authority and accountability for the information systems that process, store, or transmit the information assets. System owners are responsible for ensuring that the information systems comply with the security requirements and controls defined by the data owners and the information security manager. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 49-51, 63-64, 69-701; CISM Online Review Course, Domain 3:
Information Security Program Development and Management, Module 2: Information Security Program Framework, ISACA2

NEW QUESTION: 249
Which of the following should be the FIRST step when performing triage of a malware incident?
A. Containing the affected system
B. Preserving the forensic image
C. Comparing backup against production
D. Removing the malware
Answer: (SHOW ANSWER)
Explanation
The first step when performing triage of a malware incident is to contain the affected system, which means isolating it from the network and preventing any further communication or data transfer with the attacker or

other compromised systems. Containing the affected system helps to limit the scope and impact of the incident, preserve the evidence, and prevent the spread of the malware to other systems.
References = NIST SP 800-61 Revision 2, CISM Review Manual 15th Edition

NEW QUESTION: 250
A PRIMARY purpose of creating security policies is to:
A. define allowable security boundaries.
B. communicate management's security expectations.
C. establish the way security tasks should be executed.
D. implement management's security governance strategy.
Answer: (SHOW ANSWER)
Explanation
A security policy is a formal statement of the rules and principles that govern the protection of information assets in an organization. A security policy defines the scope, objectives, roles and responsibilities, and standards of the information security program. A primary purpose of creating security policies is to implement management's security governance strategy, which is the framework that guides the direction and alignment of information security with the business goals and objectives. A security policy translates the management's vision and expectations into specific and measurable requirements and controls that can be implemented and enforced by the information security staff and other stakeholders. A security policy also helps to establish the accountability and authority of the information security function and to demonstrate the commitment and support of the senior management for the information security program.
References =
CISM Review Manual 15th Edition, page 1631
CISM 2020: IT Security Policies2
CISM domain 1: Information security governance [Updated 2022]3
What is CISM? - Digital Guardian4

NEW QUESTION: 251
Which of the following is the MOST important reason to ensure information security is aligned with the organization's strategy?
A. To identify the organization's risk tolerance
B. To improve security processes
C. To align security roles and responsibilities
D. To optimize security risk management
Answer: (SHOW ANSWER)
Explanation
= The most important reason to ensure information security is aligned with the organization's strategy is to optimize security risk management. Information security is not an isolated function, but rather an integral part of the organization's overall objectives, processes, and governance. By aligning information security with the organization's strategy, the information security manager can ensure that security risks are identified, assessed, treated, and monitored in a consistent, effective, and efficient manner1. Alignment also enables the

information security manager to communicate the value and benefits of information security to senior management and other stakeholders, and to justify the allocation of resources and investments for security initiatives2. Alignment also helps to establish clear roles and responsibilities for information security across the organization, and to foster a culture of security awareness and accountability3. Therefore, alignment is essential for optimizing security risk management, which is the process of balancing the protection of information assets with the business objectives and risk appetite of the organization4. References = 1: CISM Exam Content Outline | CISM Certification | ISACA 2: CISM_Review_Manual Pages 1-30 - Flip PDF Download | FlipHTML5 3: CISM 2020: Information Security & Business Process Alignment 4: CISM Review Manual 15th Edition, Chapter 2, Section 2.1

NEW QUESTION: 252
An information security manager has been asked to provide both one-year and five-year plans for the information security program. What is the PRIMARY purpose for the long-term plan?
A. To facilitate the continuous improvement of the IT organization
B. To ensure controls align with security needs
C. To create and document required IT capabilities
D. To prioritize security risks on a longer scale than the one-year plan
Answer: (SHOW ANSWER)
Explanation
The primary purpose for the long-term plan for the information security program is to ensure controls align with security needs. This is because the long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. The long-term plan also facilitates the allocation and optimization of the resources and budget for the information security program, and enables the measurement and evaluation of the program's performance and value.
The long-term plan provides a strategic vision and direction for the information security program, and defines the goals, objectives, and initiatives that support the organization's mission, vision, and values. The long-term plan also helps to identify and prioritize the security risks and opportunities that may arise in the future, and to align the information security controls with the changing business and technology environment. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 3, Section 3.1.1, page 1261; CISM domain 3:
Information security program development and management [2022 update] | Infosec2; CISM: Information Security Program Development and Management Part 1 Online, Self-Paced3

NEW QUESTION: 253
Which of the following parties should be responsible for determining access levels to an application that processes client information?
A. The business client
B. The information security tear

C. The identity and access management team
D. Business unit management
Answer: (SHOW ANSWER)
Explanation
The business client should be responsible for determining access levels to an application that processes client information, because the business client is the owner of the data and the primary stakeholder of the application. The business client has the best knowledge and understanding of the business requirements, objectives, and expectations of the application, and the sensitivity, value, and criticality of the data. The business client can also define the roles and responsibilities of the users and the access rights and privileges of the users based on the principle of least privilege and the principle of separation of duties. The business client can also monitor and review the access levels and the usage of the application, and ensure that the access levels are aligned with the organization's information security policies and standards.
The information security team, the identity and access management team, and the business unit management are all involved in the process of determining access levels to an application that processes client information, but they are not the primary responsible party. The information security team provides guidance, support, and oversight to the business client on the information security best practices, controls, and standards for the application, and ensures that the access levels are consistent with the organization's information security strategy and governance. The identity and access management team implements, maintains, and audits the access levels and the access control mechanisms for the application, and ensures that the access levels are compliant with the organization's identity and access management policies and procedures. The business unit management approves, authorizes, and sponsors the access levels and the access requests for the application, and ensures that the access levels are aligned with the business unit's goals and strategies.
References = ISACA, CISM Review Manual, 16th Edition, 2020, pages 125-126, 129-130, 133-134, 137-138.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1037.

NEW QUESTION: 254
Which of the following should be the PRIMARY basis for determining the value of assets?
A. Cost of replacing the assets
B. Business cost when assets are not available
C. Original cost of the assets minus depreciation
D. Total cost of ownership (TCO)
Answer: (SHOW ANSWER)
Explanation
The primary basis for determining the value of assets should be the business cost when assets are not available. This is because the value of assets is not only determined by their acquisition or replacement cost, but also by their contribution to the organization's business objectives and processes. The business cost when assets are not available reflects the potential impact of losing or compromising the assets on the organization's operations, performance, reputation, and compliance. The business cost when assets are not available can be estimated by conducting a business impact analysis (BIA), which identifies the criticality, dependencies, and recovery requirements of the assets. By using the business cost when assets are not available as the primary

basis for determining the value of assets, the organization can prioritize the protection and management of the assets according to their importance and risk level. References = CISM Review Manual 15th Edition, page 64, page 65.

NEW QUESTION: 255
When testing an incident response plan for recovery from a ransomware attack, which of the following is MOST important to verify?
A. Digital currency is immediately available.
B. Network access requires two-factor authentication.
C. Data backups are recoverable from an offsite location.
D. An alternative network link is immediately available.
Answer: (SHOW ANSWER)
Explanation
Data backups are recoverable from an offsite location is the most important thing to verify when testing an incident response plan for recovery from a ransomware attack, as it ensures that the organization can restore its data and resume its operations without paying the ransom or losing critical information. Data backups should be performed regularly, stored securely, and tested for integrity and availability. (From CISM Review Manual
15th Edition)
References: CISM Review Manual 15th Edition, page 191, section 4.3.4.1.

NEW QUESTION: 256
While conducting a test of a business continuity plan (BCP), which of the following is the MOST important consideration?
A. The test is scheduled to reduce operational impact.
B. The test involves IT members in the test process.
C. The test addresses the critical components.
D. The test simulates actual prime-time processing conditions.
Answer: (SHOW ANSWER)
Explanation
The test addresses the critical components is the most important consideration while conducting a test of a business continuity plan (BCP), as it ensures that the test covers the essential functions, processes, and resources that are required to maintain or resume the organization's operations in the event of a disruption. The test should also verify that the recovery objectives, such as recovery time objective (RTO) and recovery point objective (RPO), are met. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1; CISSP Exam Cram: Business Continuity and Disaster Recovery Planning1, page 5, section Testing the Plan.

NEW QUESTION: 257
The information security manager has been notified of a new vulnerability that affects key data processing systems within the organization Which of the following should be done FIRST?
A. Inform senior management
B. Re-evaluate the risk
C. Implement compensating controls
D. Ask the business owner for the new remediation plan
Answer: (SHOW ANSWER)
Explanation
The first step when a new vulnerability is identified is to re-evaluate the risk associated with the vulnerability. This may require an update to the risk assessment and the implementation of additional controls. Informing senior management of the vulnerability is important, but should not be the first step. Implementing compensating controls may also be necessary, but again, should not be the first step. Asking the business owner for a remediation plan may be useful, but only after the risk has been re-evaluated.
The information security manager should first re-evaluate the risk posed by the new vulnerability to determine its impact and likelihood. Based on this assessment, appropriate actions can be taken such as informing senior management, implementing compensating controls, or requesting a remediation plan from the business owner. The other choices are possible actions but not necessarily the first one.
A vulnerability is a weakness that can be exploited by an attacker to compromise a system or network2. A vulnerability can affect key data processing systems within an organization if it exposes sensitive information, disrupts business operations, or damages assets2. A vulnerability assessment is a process of identifying and evaluating vulnerabilities and their potential consequences2

NEW QUESTION: 258
To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:
A. rely on senior management to enforce security.
B. promote the relevance and contribution of security.
C. focus on compliance.
D. reiterate the necessity of security.
Answer: (SHOW ANSWER)
Explanation
To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security to the organization's goals and

objectives. Security is not only a technical function, but also a business enabler that supports the organization's strategy, vision, and mission. By promoting the relevance and contribution of security, the information security manager can demonstrate the value and benefits of security to the stakeholders, such as increasing customer trust, enhancing reputation, reducing costs, improving efficiency, and complying with regulations. Promoting the relevance and contribution of security can also help the information security manager to build relationships and partnerships with the business units, and to align the security program with the business needs and expectations. Promoting the relevance and contribution of security can also help the information security manager to foster a positive security culture and awareness within the organization, and to encourage the adoption and support of security policies and practices.
The other options are not the best ways to overcome the perception that security is a hindrance to business activities. Relying on senior management to enforce security is not the best way, because it may create a sense of coercion and resentment among the employees, and may undermine the credibility and authority of the information security manager. Focusing on compliance is not the best way, because it may create a false sense of security and satisfaction, and may neglect the other aspects and dimensions of security, such as risk management, value creation, and innovation. Reiterating the necessity of security is not the best way, because it may not address the root causes and factors of the negative perception, and may not provide sufficient evidence and justification for the security investments and decisions. References = CISM Review Manual, 16th Edition, ISACA, 2020, pp. 13-14, 23-241; CISM Online Review Course, Domain 1: Information Security Governance, Module 1: Information Security Governance Overview, ISACA2 To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to promote the relevance and contribution of security. By demonstrating the value that security brings to the organization, including protecting assets and supporting business objectives, the information security manager can help to change the perception of security from a hindrance to a critical component of business success.
Relying on senior management to enforce security, focusing on compliance, and reiterating the necessity of security are all important elements of a comprehensive security program, but they do not directly address the perception that security is a hindrance to business activities. By promoting the relevance and contribution of security, the information security manager can help to align security with the overall goals and objectives of the organization, and foster a culture that values and supports security initiatives.

NEW QUESTION: 259
To support effective risk decision making, which of the following is MOST important to have in place?
A. Established risk domains
B. Risk reporting procedures
C. An audit committee consisting of mid-level management
D. Well-defined and approved controls
Answer: (SHOW ANSWER)
Explanation
To support effective risk decision making, it is most important to have risk reporting procedures in place. Risk reporting procedures define how, when, and to whom risk information is communicated within the organization. Risk reporting procedures ensure that risk information is timely, accurate, consistent, and relevant for the decision makers. Risk reporting procedures also facilitate the monitoring and review of risk management

activities and outcomes. Risk reporting procedures enable the organization to align its risk appetite and tolerance with its business objectives and strategies. Established risk domains are not the most important factor for effective risk decision making. Risk domains are categories or areas of risk that reflect the organization's structure, objectives, and operations. Risk domains help to organize and prioritize risk information, but they do not necessarily support the communication and analysis of risk information for decision making. An audit committee consisting of mid-level management is not the most important factor for effective risk decision making. An audit committee is a subcommittee of the board of directors that oversees the internal and external audit functions of the organization. An audit committee should consist of independent and qualified members, preferably from the board of directors or senior management, not mid-level management. An audit committee provides assurance and oversight on the effectiveness of risk management, but it does not directly support risk decision making. Well-defined and approved controls are not the most important factor for effective risk decision making. Controls are measures or actions that reduce the likelihood or impact of risk events. Well-defined and approved controls are essential for implementing risk responses and mitigating risks, but they do not directly support the identification, analysis, and evaluation of risks for decision making. References = CISM Review Manual 15th Edition, page 207-208.
Established risk domains are important for effective risk decision making because they provide a basis for categorizing risks and assessing their impact on the organization. Risk domains are also used to assign risk ownership and prioritize risk management activities. Having established risk domains in place helps ensure that risks are properly identified and addressed, and enables organizations to make informed and effective decisions about risk. Risk reporting procedures, an audit committee consisting of mid-level management, and well-defined and approved controls are all important components of an effective risk management program, but established risk domains are the most important for effective risk decision making.

NEW QUESTION: 260

Which of the following is the MOST effective way to determine the alignment of an information security program with the business strategy?

A. Evaluate the results of business continuity testing.
B. Review key performance indicators (KPIs).
C. Evaluate the business impact of incidents.
D. Engage business process owners.
Answer: (SHOW ANSWER)
Explanation
The most effective way to determine the alignment of an information security program with the business strategy is D. Engage business process owners. This is because business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. Engaging business process owners can also help to establish trust, collaboration, and communication between the information security function and the business units, and foster a culture of security awareness and accountability.

Business process owners are the key stakeholders who are responsible for defining, executing, and monitoring the business processes that support the organization's mission, vision, and goals. By engaging them, the information security manager can understand their needs, expectations, and challenges, and ensure that the information security program is aligned with their requirements and objectives. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 201; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 78, page 20

NEW QUESTION: 261
The PRIMARY advantage of single sign-on (SSO) is that it will:
A. increase efficiency of access management
B. increase the security of related applications.
C. strengthen user passwords.
D. support multiple authentication mechanisms.
Answer: A (LEAVE A REPLY)
Explanation
Single sign-on (SSO) is a technology that allows users to access multiple applications or services with one set of credentials, such as a username and password. The primary advantage of SSO is that it increases the efficiency of access management, as it reduces the need for users to remember and enter multiple passwords for different applications or services. SSO also simplifies the user experience, as they can log in once and access multiple resources without having to switch between different windows or tabs. SSO can also improve the security of related applications, as it reduces the risk of password compromise or phishing attacks. However, SSO does not strengthen user passwords or support multiple authentication mechanisms by itself. It is a complementary technology that enhances the security and convenience of access management. References = CISM Review Manual, 16th Edition, page 991 The primary advantage of single sign-on (SSO) is that it increases the efficiency of access management. With SSO, users only need to remember one set of credentials to access all of their applications, rather than having to remember multiple usernames and passwords for each application. This simplifies the user experience and helps to reduce the amount of time spent managing access to multiple applications. Additionally, SSO can also increase the security of related applications, as users are not sharing the same credentials across multiple applications, and it can also support multiple authentication mechanisms, such as biometric authentication.

NEW QUESTION: 262
Which of the following is the BEST way to help ensure an organization's risk appetite will be considered as part of the risk treatment process?
A. Establish key risk indicators (KRIs).
B. Use quantitative risk assessment methods.
C. Provide regular reporting on risk treatment to senior management
D. Require steering committee approval of risk treatment plans.
Answer: (SHOW ANSWER)
Explanation

= Requiring steering committee approval of risk treatment plans is the best way to help ensure an organization's risk appetite will be considered as part of the risk treatment process because the steering committee is composed of senior management and key stakeholders who are responsible for defining and communicating the risk appetite and ensuring that it is aligned with the business objectives and strategy. The steering committee can review and approve the risk treatment plans proposed by the information security manager and ensure that they are consistent with the risk appetite and the risk tolerance levels. The steering committee can also monitor and evaluate the effectiveness of the risk treatment plans and provide feedback and guidance to the information security manager. Establishing key risk indicators (KRIs), using quantitative risk assessment methods, and providing regular reporting on risk treatment to senior management are not the best ways to help ensure an organization's risk appetite will be considered as part of the risk treatment process, although they may be useful tools and techniques to support the risk management process. KRIs are metrics that measure the level of risk exposure and the performance of risk controls. Quantitative risk assessment methods are techniques that use numerical values and probabilities to estimate the likelihood and impact of risk events. Regular reporting on risk treatment to senior management is a way to communicate the status and results of the risk treatment process and to obtain feedback and support from senior management. However, none of these methods can ensure that the risk treatment plans are approved and aligned with the risk appetite, which is the role of the steering committee. References = CISM Review Manual 2023, Chapter 2, Section
2.4.3, page 76; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, Question ID: 121.

NEW QUESTION: 263
An information security manager is MOST likely to obtain approval for a new security project when the business case provides evidence of:
A. organizational alignment
B. IT strategy alignment
C. threats to the organization
D. existing control costs
Answer: A (LEAVE A REPLY)
Explanation
A new security project is more likely to be approved if it aligns with the organization's goals, objectives, and strategies. This shows that the project supports the business needs and adds value to the organization. Organizational alignment is one of the key elements of a business case for information security, as stated in the CISM Review Manual, 16th Edition1, page 41. IT strategy alignment, threats to the organization, and existing control costs are also important factors to consider, but they are not as persuasive as organizational alignment in obtaining approval for a new security project. References = 1: CISM Review Manual, 16th Edition by Isaca (Author) Learn more:
1. isaca.org2. amazon.com3. gov.uk

NEW QUESTION: 264

Which of the following should be considered FIRST when recovering a compromised system that needs a complete rebuild?

A. Patch management files

B. Network system logs

C. Configuration management files

D. Intrusion detection system (IDS) logs

Answer: (SHOW ANSWER)

Explanation

Patch management files are the files that contain the patches or updates for the software applications and systems that are installed on the compromised system. Patch management files are essential to recover a compromised system that needs a complete rebuild, as they can help to restore the functionality, security, and performance of the system. Without patch management files, the system may not be able to run properly or securely, and may expose the organization to further risks or vulnerabilities. Network system logs, configuration management files, and intrusion detection system (IDS) logs are also important for recovering a compromised system, but they should be considered after patch management files. Network system logs can help to identify the source and scope of the attack, configuration management files can help to restore the original settings and policies of the system, and IDS logs can help to detect any malicious activities or anomalies on the system. References = CISM Review Manual, 16th Edition, pages 193-1941; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 672

NEW QUESTION: 265

Spoofing should be prevented because it may be used to:

A. gain illegal entry to a secure system by faking the sender's address,

B. predict which way a program will branch when an option is presented

C. assemble information, track traffic, and identify network vulnerabilities.

D. capture information such as passwords traveling through the network

Answer: (SHOW ANSWER)

Explanation

Gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented. Spoofing is a technique that involves impersonating someone or something else to deceive or manipulate the recipient or target. Spoofing can be applied to various communication channels, such as emails, websites, phone calls, IP addresses, or DNS servers. One of the common goals of spoofing is to gain unauthorized access to a secure system by faking the sender's address, such as an email address or an IP address. For example, an attacker may spoof an email address of a trusted person or organization and send a phishing email that contains a malicious link or attachment. If the recipient clicks on the link or opens the attachment, they may be redirected to a fake website that asks for their credentials or downloads malware onto their device. Alternatively, an attacker may spoof an IP address of a trusted source and send packets to a secure system that contains malicious code or commands. If the system accepts the packets as legitimate, it may execute the code or commands and compromise its security. Therefore, gaining illegal entry to a secure system by faking the sender's address is one of the reasons why spoofing should be prevented.

References:

https://www.kaspersky.com/resource-center/definitions/spoofing
https://www.cisa.gov/resources-tools/resources/business-case-security
https://www.avast.com/c-spoofing

NEW QUESTION: 266
Which of the following BEST enables an information security manager to obtain organizational support for the implementation of security controls?
A. Conducting periodic vulnerability assessments
B. Communicating business impact analysis (BIA) results
C. Establishing effective stakeholder relationships
D. Defining the organization's risk management framework
Answer: (SHOW ANSWER)
Explanation
The best way to obtain organizational support for the implementation of security controls is to establish effective stakeholder relationships. Stakeholders are the individuals or groups that have an interest or influence in the organization's information security objectives, activities, and outcomes. They may include senior management, business owners, users, customers, regulators, auditors, vendors, and others. By establishing effective stakeholder relationships, the information security manager can communicate the value and benefits of security controls to the organization's performance, reputation, and competitiveness. The information security manager can also solicit feedback and input from stakeholders to ensure that the security controls are aligned with the organization's needs and expectations. The information security manager can also foster collaboration and cooperation among stakeholders to facilitate the implementation and operation of security controls. The other options are not the best way to obtain organizational support for the implementation of security controls, although they may be some steps or outcomes of the process. Conducting periodic vulnerability assessments is a technical activity that can help identify and prioritize the security weaknesses and gaps in the organization's information assets and systems. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are communicated and justified to the stakeholders. Communicating business impact analysis (BIA) results is a reporting activity that can help demonstrate the potential consequences of disruptions or incidents on the organization's critical business processes and functions. However, it does not necessarily obtain organizational support for the implementation of security controls unless the results are linked to the organization's risk appetite and tolerance. Defining the organization's risk management framework is a strategic activity that can help establish the policies, procedures, roles, and responsibilities for managing information security risks in a consistent and effective manner. However, it does not necessarily obtain organizational support for the implementation of security controls unless the framework is endorsed and enforced by the stakeholders

NEW QUESTION: 267
Which of the following events is MOST likely to require an organization to revisit its information security framework?
A. New services offered by IT
B. Changes to the risk landscape

C. A recent cybersecurity attack
D. A new technology implemented
Answer: (SHOW ANSWER)
Explanation
Changes to the risk landscape are the most likely events to require an organization to revisit its information security framework, because they may affect the organization's risk appetite, risk tolerance, risk profile, and risk treatment strategies. The information security framework should be aligned with the organization's business objectives and risk management approach, and should be reviewed and updated regularly to reflect the changing internal and external environment.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 35: "The information security framework should be reviewed and updated regularly to ensure that it remains aligned with the enterprise's business objectives and risk management approach and reflects the changing internal and external environment." CISM Review Manual, 16th Edition, ISACA, 2020, p. 36: "Changes in the risk landscape may require the enterprise to revisit its risk appetite, risk tolerance, risk profile, and risk treatment strategies."

NEW QUESTION: 268
An organization that conducts business globally is planning to utilize a third-party service provider to process payroll information. Which of the following issues poses the GREATEST risk to the organization?
A. The third party does not have an independent assessment of controls available for review.
B. The third party has not provided evidence of compliance with local regulations where data is generated.
C. The third-party contract does not include an indemnity clause for compensation in the event of a breach.
D. The third party's service level agreement (SLA) does not include guarantees of uptime.
Answer: (SHOW ANSWER)
Explanation
The third party's lack of compliance with local regulations poses the greatest risk to the organization, as it may expose the organization to legal, regulatory, or reputational consequences, such as fines, sanctions, lawsuits, or loss of customer trust. Payroll information is considered sensitive personal data that may be subject to different privacy and security laws depending on the jurisdiction where it is generated, processed, or stored. Therefore, the organization should ensure that the third party adheres to the applicable regulations and standards, and obtains the necessary certifications or attestations to demonstrate compliance.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Ensuring Vendor Compliance and Third-Party Risk Mitigation; How to Manage Access Risk Regarding Third-Party Service Providers

NEW QUESTION: 269
The categorization of incidents is MOST important for evaluating which of the following?
A. Appropriate communication channels
B. Allocation of needed resources
C. Risk severity and incident priority
D. Response and containment requirements

Answer: (SHOW ANSWER)

Explanation

The categorization of incidents is most important for evaluating the risk severity and incident priority, as these factors determine the impact and urgency of the incident, and the appropriate level of response and escalation. The categorization of incidents helps to classify the incidents based on their type, source, cause, scope, and affected assets or services. By categorizing incidents, the information security manager can assess the potential or actual harm to the organization, its stakeholders, and its objectives, and assign a priority level that reflects the need for immediate action and resolution. The risk severity and incident priority also influence the allocation of resources, the response and containment requirements, and the communication channels, but they are not the primary purpose of categorization.

References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.4.1, page 2371; CISM Online Review Course, Module 4, Lesson 4, Topic 12; CIRT Case Classification (Draft) - FIRST3

NEW QUESTION: 270

Which of the following BEST demonstrates the added value of an information security program?

A. Security baselines

B. A gap analysis

C. A SWOT analysis

D. A balanced scorecard

Answer: (SHOW ANSWER)

Explanation

A balanced scorecard is a tool that can be used to demonstrate the added value of an information security program by measuring and reporting on key performance indicators (KPIs) and key risk indicators (KRIs) aligned with strategic objectives. Security baselines, a gap analysis and a SWOT analysis are all useful for assessing and improving security posture, but they do not necessarily show how security contributes to business value.

NEW QUESTION: 271

A balanced scorecard MOST effectively enables information security:

A. project management

B. governance.

C. performance.

D. risk management.

Answer: (SHOW ANSWER)

Explanation

A balanced scorecard most effectively enables information security govern-ance. Information security governance is the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations, and are managed effectively and efficiently1. A balanced scorecard is a tool for meas-uring and communicating the performance and progress of an organization toward its strategic goals. It typically includes

four perspectives: financial, customer, internal pro-cess, and learning and growth2. A balanced scorecard can help information security managers to:
*Align information security objectives with business objectives and communicate them to senior management and other stakeholders
*Monitor and report on the effectiveness and efficiency of information security processes and controls
*Identify and prioritize improvement opportunities and corrective actions
*Demonstrate the value and benefits of information security investments
*Foster a culture of security awareness and continuous learning
Several sources have proposed models or frameworks for applying the balanced scorecard approach to information security governance34 . The other options are not the most effective applications of a balanced scorecard for information security. Pro-ject management is the process of planning, executing, monitoring, and closing pro-jects to achieve specific objectives within constraints such as time, budget, scope, and quality. A balanced scorecard can be used to measure the performance of individual projects or project portfolios, but it is not specific to information security projects. Per-formance is the degree to which an organization or a process achieves its objectives or meets its standards. A balanced scorecard can be used to measure the performance of information security processes or functions, but it is not limited to performance measurement. Risk management is the process of identifying, analyzing, evaluating, treating, monitoring, and communicating risks that affect an organization's objec-tives. A balanced scorecard can be used to measure the risk exposure and risk appetite of an organization, but it is not a tool for risk assessment or treatment.
References: 1: Information Security Governance - ISACA 2: Balanced scorecard - Wikipedia 3: Key Per-formance Indicators for Security Governance Part 1 - ISACA 4: A Strategy Map for Se-curity Leaders: Applying the Balanced Scorecard Framework to Information Security - Security Intelligence : How to Measure Security From a Governance Perspective - ISA-CA : Project management - Wikipedia : Performance measurement - Wikipedia : Risk management - Wikipedia

NEW QUESTION: 272
Which of the following should include contact information for representatives of equipment and software vendors?
A. Information security program charter
B. Business impact analysis (BIA)
C. Service level agreements (SLAs)
D. Business continuity plan (BCP)
Answer: D (LEAVE A REPLY)

Explanation
The document that should include contact information for representatives of equipment and software vendors is the business continuity plan (BCP) because it provides the guidance and procedures for restoring the organization's critical business functions and operations in the event of a disruption or disaster, and may require contacting external parties such as vendors for assistance or support. Information security program charter is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Business impact analysis (BIA) is not a good document for this purpose because it does not provide any guidance or procedures for business continuity or disaster recovery. Service level agreements (SLAs) are not good documents for this purpose because they do not provide any guidance or procedures for business continuity or disaster recovery. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/business-continuity-management-lifecycle
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/business-impact-analysis

NEW QUESTION: 273
Which of the following defines the triggers within a business continuity plan (BCP)? @
A. Needs of the organization
B. Disaster recovery plan (DRP)
C. Information security policy
D. Gap analysis
Answer: (SHOW ANSWER)
Explanation
The needs of the organization define the triggers within a business continuity plan (BCP). Triggers are the events or conditions that initiate the activation of the BCP. The triggers should be based on the organization's business objectives, risk appetite, recovery time objectives, and recovery point objectives. The triggers should also be aligned with the organization's information security policy, disaster recovery plan, and gap analysis. However, these are not the primary factors that define the triggers, but rather the supporting elements that help implement the BCP. The needs of the organization are the main drivers for determining the triggers, as they reflect the organization's priorities, expectations, and requirements for business continuity. References = CISM Review Manual (Digital Version) 1, Chapter 4: Information Security Incident Management, pages 191-192, 195-196, 199-200.
Business Continuity Management Guideline 2, page 5, Section 4.2.1: Triggers Business Continuity Plan - Open Risk Manual 3, page 1, Section 1: Introduction

NEW QUESTION: 274
Which of the following is the BEST way to help ensure alignment of the information security program with organizational objectives?
A. Establish an information security steering committee.
B. Employ a process-based approach for information asset classification.
C. Utilize an industry-recognized risk management framework.
D. Provide security awareness training to board executives.
Answer: (SHOW ANSWER)

Explanation
The best way to help ensure alignment of the information security program with organizational objectives is A. Establish an information security steering committee. This is because an information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. An information security steering committee can help to ensure that the information security program is aligned with the organizational objectives by: Communicating and promoting the vision, mission, and value of information security to the organization and its stakeholders Defining and approving the information security policies, standards, and procedures Establishing and monitoring the information security goals, metrics, and performance indicators Allocating and prioritizing the resources and budget for information security initiatives and projects Resolving any conflicts or issues that may arise between the information security function and the business units Reviewing and endorsing the information security risk assessment and treatment plans Ensuring compliance with the legal, regulatory, and contractual obligations regarding information security An information security steering committee is a cross-functional group of senior executives and managers who provide strategic direction, oversight, and support for the information security program. (From CISM Manual or related resources) References = CISM Review Manual 15th Edition, Chapter 1, Section 1.2.2, page 20; CISM Review Questions, Answers & Explanations Manual 9th Edition, Question 9, page 3; Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

NEW QUESTION: 275
During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?
A. Post-incident review
B. Eradication
C. Containment
D. Identification
Answer: (SHOW ANSWER)
Explanation
The eradication phase of incident response is the stage where the incident response team documents and performs the actions required to remove the threat that caused the incident1. This phase involves identifying and eliminating the root cause of the incident, such as malware, compromised accounts, unauthorized access, or misconfigured systems2. The eradication phase also involves restoring the affected systems to a secure state, deleting any malicious files or artifacts, and verifying that the threat has been completely removed2. The eradication phase is the first step in returning a compromised environment to its proper state2. The other phases of incident response are:
Preparation: The phase where the incident response team prepares for potential incidents by defining roles, responsibilities, procedures, tools, and resources1.
Detection and analysis: The phase where the incident response team identifies and prioritizes the incidents based on their severity, impact, and urgency1.
Containment: The phase where the incident response team isolates the affected systems or networks to prevent the spread of the incident and minimize the damage1.

Recovery: The phase where the incident response team restores the normal operations of the systems or networks, and implements any necessary changes or improvements to prevent recurrence1.
Post-incident review: The phase where the incident response team evaluates the effectiveness of the incident response process, identifies the lessons learned, and provides recommendations for improvement1.
References = 3: Critical Incident Stress Management: CISM Implementation Guidelines 2: What is the Eradication Phase of Incident Response? - RSI Security 1: Incident Response Models - ISACA

NEW QUESTION: 276
Which of the following is MOST important when developing an information security strategy?
A. Engage stakeholders.
B. Assign data ownership.
C. Determine information types.
D. Classify information assets.
Answer: (SHOW ANSWER)
Explanation
According to the CISM Review Manual, engaging stakeholders is the most important step when developing an information security strategy, as it helps to ensure that the strategy is aligned with the business objectives, expectations, and requirements of the stakeholders. Engaging stakeholders also helps to gain their support and commitment for the implementation and maintenance of the strategy. Assigning data ownership, determining information types, and classifying information assets are possible subsequent steps, but not the most important one.
References = CISM Review Manual, 27th Edition, Chapter 2, Section 2.1.1, page 731.

NEW QUESTION: 277
Which of the following should be an information security manager's FIRST course of action when one of the organization's critical third-party providers experiences a data breach?
A. Inform the public relations officer.
B. Inform customers of the breach.
C. Invoke the incident response plan.
D. Monitor the third party's response.
Answer: (SHOW ANSWER)
Explanation
The information security manager's first course of action when one of the organization's critical third-party providers experiences a data breach should be to invoke the incident response plan that has been established for such scenarios. The incident response plan should define the roles and responsibilities, communication channels, escalation procedures, and recovery actions for dealing with a third-party data breach. Invoking the incident response plan will help to contain the impact, assess the damage, coordinate the response, and restore the normal operations as soon as possible.
References = CISM Review Manual, 16th Edition, page 290

NEW QUESTION: 278

The MAIN reason for having senior management review and approve an information security strategic plan is to ensure:

A. the organization has the required funds to implement the plan.

B. compliance with legal and regulatory requirements.

C. staff participation in information security efforts.

D. the plan aligns with corporate governance.

Answer: (SHOW ANSWER)

Explanation

The main reason for having senior management review and approve an information security strategic plan is to ensure that the plan aligns with the corporate governance of the organization. Corporate governance is the set of responsibilities and practices exercised by the board and executive management to provide strategic direction, ensure objectives are achieved, manage risks appropriately and verify that the organization's resources are used responsibly1. An information security strategic plan is a document that defines the vision, mission, goals, objectives, scope and approach for the information security program of the organization2. The plan should be aligned with the organization's business strategy, risk appetite, culture, values and objectives3. By reviewing and approving the plan, senior management demonstrates their commitment and support for the information security program, ensures its alignment with the corporate governance, and provides the necessary resources and authority for its implementation4. References = 1: CISM Review Manual 15th Edition, ISACA, 2017, page 172: CISM Review Manual 15th Edition, ISACA, 2017, page 253: CISM Review Manual 15th Edition, ISACA, 2017, page 264: CISM Review Manual 15th Edition, ISACA, 2017, page 27.

Senior management review and approval of an information security strategic plan is important to ensure that the plan is aligned with the organization's overall corporate governance objectives. It is also important to ensure that the plan takes into account any legal and regulatory requirements, as well as the resources and staff needed to properly implement the plan.

NEW QUESTION: 279

Which of the following would provide the MOST effective security outcome in an organizations contract management process?

A. Performing vendor security benchmark analyses at the request-for-proposal (RFP) stage

B. Ensuring security requirements are defined at the request-for-proposal (RFP) stage

C. Extending security assessment to cover asset disposal on contract termination

D. Extending security assessment to include random penetration testing

Answer: (SHOW ANSWER)

Explanation

Ensuring security requirements are defined at the request-for-proposal (RFP) stage is the most effective security outcome in an organization's contract management process because it establishes and communicates the security expectations and obligations for both parties, and enables the organization to evaluate and select the most suitable and secure vendor or service provider. Performing vendor security benchmark analyses at the RFP stage is not an effective security outcome, but rather a possible security activity that involves

comparing and ranking different vendors or service providers based on their security capabilities or performance.
Extending security assessment to cover asset disposal on contract termination is not an effective security outcome, but rather a possible security activity that involves verifying and validating that any assets or data belonging to the organization are securely disposed of by the vendor or service provider at the end of the contract. Extending security assessment to include random penetration testing is not an effective security outcome, but rather a possible security activity that involves testing and auditing the vendor's or service provider's security controls or systems at random intervals during the contract. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/data-ownership-and-custodianship-in-the-cl
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/integrating-assurance-functions

NEW QUESTION: 280
A business impact analysis (BIA) should be periodically executed PRIMARILY to:
A. validate vulnerabilities on environmental changes.
B. analyze the importance of assets.
C. check compliance with regulations.
D. verify the effectiveness of controls.
Answer: (SHOW ANSWER)
Explanation
A business impact analysis (BIA) is a process that helps identify and evaluate the potential effects of disruptions or incidents on the organization's mission, objectives, and operations. A BIA should be periodically executed to verify the effectiveness of the controls that are implemented to prevent, mitigate, or recover from such disruptions or incidents12.
According to the CISM Manual, a BIA should be performed at least annually for critical systems and processes, and more frequently for non-critical ones3. A BIA should also be updated whenever there are significant changes in the organization's environment, such as new regulations, technologies, business models, or stakeholder expectations3. A BIA should not be used to validate vulnerabilities on environmental changes (A), analyze the importance of assets (B), or check compliance with regulations , as these are not the primary purposes of a BIA.
References: 1: IR 8286D, Using Business Impact Analysis to Inform Risk Prioritization and Response | CSRC NIST 2: CISM Domain 4 Preview | BCP - Business Impact Analysis (BIA) - YouTube 3: CISM ITEM DEVELOPMENT GUIDE - ISACA

NEW QUESTION: 281
Which of the following provides the BEST evidence that a recently established infofmation security program is effective?
A. The number of reported incidents has increased
B. Regular IT balanced scorecards are communicated.
C. Senior management has reported fewer junk emails.
D. The number of tickets associated with IT incidents have stayed consistent

Answer: (SHOW ANSWER)

Explanation

The number of reported incidents has increased is the best evidence that a recently established information security program is effective because it indicates that the organization has improved its detection and reporting capabilities and has raised awareness among employees about security issues. Regular IT balanced scorecards are communicated is not a good evidence because it does not measure the actual performance or outcomes of the security program. Senior management has reported fewer junk emails is not a good evidence because it does not reflect the overall security posture or maturity of the organization. The number of tickets associated with IT incidents have stayed consistent is not a good evidence because it does not show any improvement or reduction in security incidents or risks. References:

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-inform

https://www.isaca.org/resources/isaca-journal/issues/2014/volume-6/how-to-measure-the-effectiveness-of-your-i

NEW QUESTION: 282

An information security manager is working to incorporate media communication procedures into the security incident communication plan. It would be MOST important to include:

A. a directory of approved local media contacts

B. pre-prepared media statements

C. procedures to contact law enforcement

D. a single point of contact within the organization

Answer: (SHOW ANSWER)

Explanation

A single point of contact within the organization is the most important element to include when incorporating media communication procedures into the security incident communication plan because it helps to ensure a consistent and accurate message to the public and avoid confusion or misinformation. A single point of contact is a designated person who is authorized and trained to communicate with the media on behalf of the organization during a security incident. The single point of contact should coordinate with the incident response team, senior management, legal counsel, and public relations to prepare and deliver timely and appropriate statements to the media, as well as to respond to any inquiries or requests. A single point of contact also helps to prevent unauthorized or conflicting disclosures from other employees or stakeholders that may harm the organization's reputation or legal position. Therefore, a single point of contact within the organization is the correct answer.

References:

https://www.lifars.com/2020/09/communication-during-incident-response/

https://ifpo.org/resource-links/articles-and-reports/public-and-media-relations/planning-for-effective-medi

https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a-communication-pla

NEW QUESTION: 283

Which of the following is the BEST justification for making a revision to a password policy?

A. Industry best practice
B. A risk assessment
C. Audit recommendation
D. Vendor recommendation
Answer: (SHOW ANSWER)
Explanation
A risk assessment should be conducted in order to identify the potential risks associated with a particular system or process, and to determine the best way to mitigate those risks. Making a revision to a password policy based on the results of a risk assessment is the best way to ensure that the policy is effective and secure.
According to the Certified Information Security Manager (CISM) Study manual, the BEST justification for making a revision to a password policy is a risk assessment. A risk assessment enables an organization to identify and evaluate the risks to its information assets and determine the appropriate measures to mitigate those risks, including password policies. Password policies should be based on the risks to the organization's information assets and the level of protection needed.

NEW QUESTION: 284
In an organization with a rapidly changing environment, business management has accepted an information security risk. It is MOST important for the information security manager to ensure:
A. change activities are documented.
B. the rationale for acceptance is periodically reviewed.
C. the acceptance is aligned with business strategy.
D. compliance with the risk acceptance framework.
Answer: (SHOW ANSWER)
Explanation
= In an organization with a rapidly changing environment, the information security risk landscape may also change frequently due to new threats, vulnerabilities, impacts, or controls. Therefore, the information security manager should ensure that the risk acceptance decisions made by the business management are periodically reviewed to verify that they are still valid and aligned with the current risk appetite and tolerance of the organization. The rationale for acceptance should be documented and updated as necessary to reflect the changes in the risk environment and the business objectives. The information security manager should also monitor the accepted risks and report any deviations or issues to the business management and the senior management.
References =
CISM Review Manual 15th Edition, page 1131
CISM Review Questions, Answers & Explanations Manual 9th Edition, page 482 CISM Domain 2: Information Risk Management (IRM) [2022 update]3

NEW QUESTION: 285
Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements?

A. Alive demonstration of the third-party supplier's security capabilities
B. The ability to i third-party supplier's IT systems and processes
C. Third-party security control self-assessment (CSA) results
D. An independent review report indicating compliance with industry standards
Answer: B (LEAVE A REPLY)
Explanation
A service provider is a third-party supplier that provides IT services or products to an organization. A service provider should comply with the organization's information security requirements, such as policies, standards, procedures, and controls, to ensure the confidentiality, integrity, and availability of the organization's data and systems. The best way to provide an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements is to have the ability to audit the third-party supplier's IT systems and processes. An audit is a systematic and independent examination of evidence to determine the degree of conformity to predetermined criteria. An audit can verify the effectiveness and efficiency of the service provider's security controls, identify any gaps or weaknesses, and provide recommendations for improvement. An audit can also ensure that the service provider adheres to the contractual obligations and service level agreements (SLAs) with the organization. Therefore, option B is the most appropriate answer.
Option A is not the best answer because a live demonstration of the third-party supplier's security capabilities may not be comprehensive, objective, or reliable. A live demonstration may only show the positive aspects of the service provider's security, but not reveal any hidden or potential issues. A live demonstration may also be subject to manipulation or deception by the service provider.
Option C is not the best answer because third-party security control self-assessment (CSA) results may not be accurate, complete, or consistent. A self-assessment is a process where the service provider evaluates its own security controls against a set of criteria or standards. A self-assessment may be biased, subjective, or incomplete, as the service provider may not disclose or report all the relevant information or issues. A self-assessment may also vary in quality and scope depending on the service provider's expertise, resources, and methodology.
Option D is not the best answer because an independent review report indicating compliance with industry standards may not be sufficient or specific for the organization's information security requirements. An independent review is a process where an external party evaluates the service provider's security controls against a set of industry standards or best practices, such as ISO/IEC 27001, NIST CSF, PCI DSS, etc. An independent review report may provide a general overview of the service provider's security posture, but not address the organization's unique or specific security needs, risks, or expectations. An independent review report may also be outdated, limited, or generic, as the industry standards or best practices may not reflect the current or emerging security threats or trends. References = CISM Review Manual 15th Edition1, pages 257-258; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 301.
An independent review report indicating compliance with industry standards BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements. This is because an independent review report is an objective and reliable source of evidence that the service provider has implemented and maintained effective security controls that meet the

industry standards and best practices. An independent review report can also provide assurance that the service provider has addressed any gaps or weaknesses identified in previous audits or assessments.

NEW QUESTION: 286
The fundamental purpose of establishing security metrics is to:
A. increase return on investment (ROI)
B. provide feedback on control effectiveness
C. adopt security best practices
D. establish security benchmarks
Answer: (SHOW ANSWER)
Explanation
The fundamental purpose of establishing security metrics is to provide feedback on the effectiveness of the information security controls and processes. Security metrics are quantitative or qualitative measures that indicate how well the organization is achieving its security objectives and goals. Security metrics can help the information security manager to monitor, evaluate, and improve the performance of the information security program, as well as to identify gaps, weaknesses, and areas for improvement. Security metrics can also help the organization to demonstrate compliance with internal and external standards, regulations, and best practices. Increasing return on investment (ROI), adopting security best practices, and establishing security benchmarks are possible outcomes or benefits of using security metrics, but they are not the fundamental purpose of establishing them. References = CISM Review Manual, 16th Edition, pages 46-471; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 642 Learn more:
1. isaca.org2. amazon.com3. gov.uk
Security metrics are used to measure the effectiveness of controls and evaluate the overall security posture of an organization. This feedback provides an understanding of the progress made towards achieving security objectives and allows organizations to make necessary adjustments.

NEW QUESTION: 287
The MOST important reason for having an information security manager serve on the change management committee is to:
A. identify changes to the information security policy.
B. ensure that changes are tested.
C. ensure changes are properly documented.
D. advise on change-related risk.

Answer: (SHOW ANSWER)

Explanation

The most important reason for having an information security manager serve on the change management committee is to advise on change-related risk. Change management is the process of planning, implementing, and controlling changes to the organization's IT systems, processes, or services, in order to achieve the desired outcomes and minimize the negative impacts1. Change-related risk is the possibility of adverse consequences or events resulting from the changes, such as security breaches, system failures, data loss, compliance violations, or customer dissatisfaction2.

The information security manager is responsible for ensuring that the organization's information assets are protected from internal and external threats, and that the information security objectives and requirements are aligned with the business goals and strategies3. Therefore, the information security manager should serve on the change management committee to advise on change-related risk, and to ensure that the changes are consistent with the information security policy, standards, and best practices. The information security manager can also help to identify and assess the potential security risks and impacts of the changes, and to recommend and implement appropriate security controls and measures to mitigate them. The information security manager can also help to monitor and evaluate the effectiveness and performance of the changes, and to identify and resolve any security issues or incidents that may arise from the changes4.

The other options are not as important as advising on change-related risk, because they are either more specific, limited, or dependent on the information security manager's role. Identifying changes to the information security policy is a task that the information security manager may perform as part of the change management process, but it is not the primary reason for serving on the change management committee. The information security policy is the document that defines the organization's information security principles, objectives, roles, and responsibilities, and it should be reviewed and updated regularly to reflect the changes in the organization's environment, needs, and risks5. However, identifying changes to the information security policy is not as important as advising on change-related risk, because the policy is a high-level document that does not provide specific guidance or details on how to implement or manage the changes. Ensuring that changes are tested is a quality assurance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Testing is the process of verifying and validating that the changes meet the expected requirements, specifications, and outcomes, and that they do not introduce any errors, defects, or vulnerabilities. However, ensuring that changes are tested is not as important as advising on change-related risk, because testing is a technical or operational activity that does not address the strategic or holistic aspects of change-related risk. Ensuring changes are properly documented is a governance activity that the change management committee may perform or oversee as part of the change management process, but it is not the primary reason for having an information security manager on the committee. Documentation is the process of recording and maintaining the information and evidence related to the changes, such as the change requests, approvals, plans, procedures, results, reports, and lessons learned. However, ensuring changes are properly documented is not as important as advising on change-related risk, because documentation is a procedural or administrative activity that does not provide any analysis or evaluation of change-related risk. References = 1: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 2: CISM Review Manual 15th Edition, Chapter 2, Section 2.5 3: CISM Review Manual 15th Edition, Chapter 1, Section 1.1 4: CISM Review Manual 15th Edition,

Chapter 2, Section 2.5 5: CISM Review Manual 15th Edition, Chapter 1, Section 1.3 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5 : CISM Review Manual 15th Edition, Chapter 2, Section 2.5

NEW QUESTION: 288
A risk owner has accepted a large amount of risk due to the high cost of controls. Which of the following should be the information security manager's PRIMARY focus in this situation?
A. Establishing a strong ongoing risk monitoring process
B. Presenting the risk profile for approval by the risk owner
C. Conducting an independent review of risk responses
D. Updating the information security standards to include the accepted risk
Answer: (SHOW ANSWER)
Explanation
The information security manager's PRIMARY focus in this situation should be establishing a strong ongoing risk monitoring process, which is the process of tracking and evaluating the changes in the risk environment, the effectiveness of the risk responses, and the impact of the residual risk on the organization. A strong ongoing risk monitoring process can help the information security manager to identify any deviations from the expected risk level, to report any significant changes or issues to the risk owner and other stakeholders, and to recommend any adjustments or improvements to the risk management strategy. Presenting the risk profile for approval by the risk owner is not the primary focus in this situation, as it is a step that should be done before the risk owner accepts the risk, not after. Conducting an independent review of risk responses is not the primary focus in this situation, as it is a quality assurance activity that can be performed by an external auditor or a third-party expert, not by the information security manager. Updating the information security standards to include the accepted risk is not the primary focus in this situation, as it is a documentation activity that does not address the ongoing monitoring and reporting of the risk. References = CISM Review Manual, 16th Edition, page 2281; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 1022

NEW QUESTION: 289
Which of the following has the GREATEST influence on an organization's information security strategy?
A. The organization's risk tolerance
B. The organizational structure
C. Industry security standards
D. Information security awareness
Answer: (SHOW ANSWER)
Explanation
An organization's information security strategy should be aligned with its risk tolerance, which is the level of risk that an organization is willing to accept in pursuit of its objectives. The strategy should aim to balance the cost of security controls with the potential impact of security incidents on the organization's objectives. Therefore, an organization's risk tolerance has the greatest influence on its information security strategy.
The organization's risk tolerance has the greatest influence on its information security strategy because it determines how much risk the organization is willing to accept and how much resources it will allocate to mitigate or transfer risk. The organizational structure, industry security standards, and information security

awareness are important factors that affect the implementation and effectiveness of an information security strategy but not as much as the organization's risk tolerance.
An information security strategy is a high-level plan that defines how an organization will achieve its information security objectives and address its information security risks. An information security strategy should align with the organization's business strategy and reflect its mission, vision, values, and culture. An information security strategy should also consider the external and internal factors that influence the organization's information security environment such as laws, regulations, competitors, customers, suppliers, partners, stakeholders, employees etc.

NEW QUESTION: 290

Security administration efforts will be greatly reduced following the deployment of which of the following techniques?

A. Discretionary access control
B. Role-based access control
C. Access control lists
D. Distributed access control
Answer: (SHOW ANSWER)
Explanation
Role-based access control (RBAC) is a policy-neutral access control mechanism that assigns access privileges to defined roles in the organization and then makes each user a member of the appropriate roles. RBAC reduces security administration efforts by simplifying the management of access rights across different users and resources. RBAC also enables consistent and efficient enforcement of the principle of least privilege, which grants users only the minimum rights required to perform their assigned tasks. RBAC can also facilitate the implementation of separation of duties, which prevents users from having conflicting or incompatible responsibilities. RBAC is among the most widely used methods in the information security tool kit1.
References = CIS Control 6: Access Control Management - Netwrix, CISSP certification: RBAC (Role based access control), What is RBAC? (Role Based Access Control) - IONOS

NEW QUESTION: 291
Which of the following is MOST important for the improvement of a business continuity plan (BCP)?
A. Implementing an IT resilience solution
B. Implementing management reviews
C. Incorporating lessons learned
D. Documenting critical business processes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 292
A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. The chief information security officer (CISO) should be MOST concerned with:

A. developing a security program that meets global and regional requirements.
B. ensuring effective communication with local regulatory bodies.
C. using industry best practice to meet local legal regulatory requirements.
D. monitoring compliance with defined security policies and standards.
Answer: (SHOW ANSWER)
Explanation
= A multinational organization is required to follow governmental regulations with different security requirements at each of its operating locations. This means that the CISO has to deal with multiple and diverse legal, regulatory, and compliance issues across different jurisdictions and markets. The CISO should be most concerned with developing a security program that meets global and regional requirements, such as ISO/IEC 27001, NIST CSF, PCI DSS, GDPR, etc. These standards provide a framework for establishing, implementing, maintaining, and improving an information security management system (ISMS) that aligns with the organization's business objectives and risk appetite. The CISO should also ensure that the security program is consistent and coherent across all operating locations, and that it complies with the specific regulations of each location. Therefore, option A is the most appropriate answer. References = CISM Review Manual 15th Edition, page 255; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 234.In this scenario, the chief information security officer (CISO) should be most concerned with developing a security program that meets the global and regional requirements of the organization. This includes considering the different legal and regulatory requirements of each operating location, and designing a security program that meets all of these requirements. The CISO should also ensure effective communication with local regulatory bodies to ensure compliance and understanding of the security program. Additionally, the CISO should use industry best practices and defined security policies and standards to ensure the program meets all applicable requirements.

NEW QUESTION: 293
Which of the following is MOST useful to an information security manager when determining the need to escalate an incident to senior?
A. Incident management procedures
B. Incident management policy
C. System risk assessment
D. Organizational risk register
Answer: (SHOW ANSWER)
Explanation
The organizational risk register is the most useful for an information security manager when determining the need to escalate an incident to senior management because it contains a list of identified risks to the organization, their likelihood and impact, and their predefined risk thresholds or targets, which can help the information security manager assess the severity and urgency of the incident and decide whether it requires senior management's attention or action. Incident management procedures are not very useful for this purpose because they do not provide any specific criteria or guidance on when to escalate an incident to senior management. Incident management policy is not very useful for this purpose because it does not provide any specific criteria or guidance on when to escalate an incident to senior management. System risk assessment is

not very useful for this purpose because it does not reflect the current risk exposure or status of the organization as a whole. References:
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/how-to-measure-the-effectiveness-of-inform
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/incident-response-lessons-learned

NEW QUESTION: 294
An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:
A. conduct an incident forensic analysis.
B. fallow the incident response plan
C. notify the business process owner.
D. fallow the business continuity plan (BCP).
Answer: (SHOW ANSWER)
Explanation
Before classifying the suspected event as a security incident, it is most important for the security manager to follow the incident response plan, which is a predefined set of procedures and guidelines that outline the roles, responsibilities, and actions of the incident management team and the organization in the event of a security event or incident. Following the incident response plan can help to ensure a consistent, coordinated, and effective response to the suspected event, as well as to minimize the impact and damage to the business processes, functions, and assets. Following the incident response plan can also help to determine the nature, scope, and severity of the suspected event, and to decide whether it meets the criteria and threshold for being classified as a security incident that requires further escalation, investigation, and resolution. Following the incident response plan can also help to document and report the incident details, activities, and outcomes, and to provide feedback and recommendations for improvement and optimization of the incident response process and plan.
Conducting an incident forensic analysis, notifying the business process owner, and following the business continuity plan (BCP) are all important steps in the incident response process, but they are not the most important ones before classifying the suspected event as a security incident. Conducting an incident forensic analysis is a technical and detailed process that involves collecting, preserving, analyzing, and presenting evidence related to the incident, and it is usually performed after the incident has been classified, contained, and eradicated. Notifying the business process owner is a communication and notification process that involves informing the relevant stakeholders of the incident status, impact, and actions, and it is usually performed after the incident has been classified and assessed. Following the business continuity plan (BCP) is a recovery and restoration process that involves resuming and restoring the normal business operations and functions after the incident has been resolved and lessons learned have been identified and implemented.
References = CISM Review Manual 15th Edition, pages 237-2411; CISM Practice Quiz, question 1422

NEW QUESTION: 295
Which of the following trends would be of GREATEST concern when reviewing the performance of an organization's intrusion detection systems (IDSs)?

A. Decrease in false positives
B. Increase in false positives
C. Increase in false negatives
D. Decrease in false negatives
Answer: (SHOW ANSWER)
Explanation
An increase in false negatives would be of greatest concern when reviewing the performance of an organization's IDSs, because it means that the IDSs are failing to detect and alert on actual attacks that are occurring on the network. False negatives can lead to serious security breaches, data loss, reputational damage, and legal liabilities for the organization. False positives, on the other hand, are alerts that are triggered by benign or normal activities that are mistaken for attacks. False positives can cause annoyance, inefficiency, and desensitization, but they do not pose a direct threat to the security of the network. Therefore, a decrease in false positives would be desirable, and an increase in false positives would be less concerning than an increase in false negatives.
References = CISM Review Manual, 16th Edition, page 2231; Intrusion Detection Systems | NIST

NEW QUESTION: 296
Which of the following is the BEST indication ofa successful information security culture?
A. Penetration testing is done regularly and findings remediated.
B. End users know how to identify and report incidents.
C. Individuals are given roles based on job functions.
D. The budget allocated for information security is sufficient.
Answer: B (LEAVE A REPLY)
Explanation
The best indication of a successful information security culture is that end users know how to identify and report incidents. This shows that the end users are aware of the information security policies, procedures, and practices of the organization, and that they understand their roles and responsibilities in protecting the information assets and resources. It also shows that the end users are engaged and committed to the information security goals and objectives of the organization, and that they are willing to cooperate and collaborate with the information security team and other stakeholders in preventing, detecting, and responding to information security incidents. A successful information security culture is one that fosters a positive attitude and behavior toward information security among all members of the organization, and that aligns the information security strategy with the business strategy and the organizational culture1.
References = CISM Review Manual, 16th Edition, Chapter 1: Information Security Governance, Section: Information Security Culture, page 281.

NEW QUESTION: 297
Which of the following BEST enables an information security manager to determine the comprehensiveness of an organization's information security strategy?
A. Internal security audit
B. External security audit

C. Organizational risk appetite
D. Business impact analysis (BIA)
Answer: (SHOW ANSWER)
Explanation
The organizational risk appetite is the best indicator of the comprehensiveness of an information security strategy. The risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives. The information security strategy should align with the risk appetite and provide a framework for managing the risks that the organization faces. An internal or external security audit can assess the effectiveness of the information security strategy, but not its comprehensiveness. A business impact analysis (BIA) can identify the critical business processes and assets that need to be protected, but not the overall scope and direction of the information security strategy. References = CISM Review Manual 2023, page 36 1; CISM Practice Quiz 2

NEW QUESTION: 298
Which of the following is the PRIMARY purpose of a business impact analysis (BIA)?
A. To define security roles and responsibilities
B. To determine return on investment (ROI)
C. To establish incident severity levels
D. To determine the criticality of information assets
Answer: (SHOW ANSWER)
Explanation
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident or emergency. The primary purpose of a BIA is to determine the criticality of information assets and the impact of their unavailability on the organization's mission, objectives and reputation. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 178, section 4.3.2.1.

NEW QUESTION: 299
An information security manager learns through a threat intelligence service that the organization may be targeted for a major emerging threat. Which of the following is the information security manager's FIRST course of action?
A. Conduct an information security audit.
B. Validate the relevance of the information.
C. Perform a gap analysis.
D. Inform senior management
Answer: (SHOW ANSWER)
Explanation
The information security manager's first course of action should be to validate the relevance of the information received from the threat intelligence service. This means verifying the source, credibility, accuracy, and timeliness of the information, as well as assessing the potential impact and likelihood of the threat for the organization. This will help the information security manager to determine the appropriate response and

prioritize the actions to mitigate the threat. Conducting an information security audit, performing a gap analysis, and informing senior management are possible subsequent actions, but they are not the first course of action. An information security audit is a systematic and independent assessment of the effectiveness of the information security controls and processes. A gap analysis is a comparison of the current state of the information security program with the desired state or best practices. Informing senior management is a communication activity that should be done after validating the information and assessing the risk. References = CISM Review Manual, 16th Edition, pages 44-451; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 632 The first step the information security manager should take upon learning of the potential threat is to validate the relevance of the information. This should involve researching the threat to evaluate its potential impact on the organization and to determine the accuracy of the threat intelligence. Once the information is validated, the information security manager can then take action, such as informing senior management, conducting an information security audit, or performing a gap analysis.

NEW QUESTION: 300

Which of the following BEST describes a buffer overflow?

A. A function is carried out with more data than the function can handle

B. A program contains a hidden and unintended function that presents a security risk

C. Malicious code designed to interfere with normal operations

D. A type of covert channel that captures data

Answer: A (LEAVE A REPLY)

Explanation

A buffer overflow is a software coding error or vulnerability that occurs when a function is carried out with more data than the function can handle, resulting in adjacent memory locations being overwritten or corrupted by the excess data1. A program contains a hidden and unintended function that presents a security risk is not a buffer overflow, but rather a backdoor2. Malicious code designed to interfere with normal operations is not a buffer overflow, but rather malware3. A type of covert channel that captures data is not a buffer overflow, but rather a keylogger. References: 1 https://www.fortinet.com/resources/cyberglossary/buffer-overflow 2 https://www.fortinet.com/resources/cyberglossary/backdoor 3 https://www.fortinet.com/resources/cyberglossary/malware https://www.fortinet.com/resources/cyberglossary/keylogger

NEW QUESTION: 301

After a ransomware incident an organization's systems were restored. Which of the following should be of MOST concern to the information security manager?

A. The service level agreement (SLA) was not met.

B. The recovery time objective (RTO) was not met.

C. The root cause was not identified.

D. Notification to stakeholders was delayed.

Answer: (SHOW ANSWER)

Explanation

= After a ransomware incident, the most important concern for the information security manager is to identify the root cause of the incident and prevent it from happening again. The root cause analysis (RCA) is a systematic process of finding and eliminating the underlying factors that led to the incident, such as vulnerabilities, misconfigurations, human errors, or malicious actions. Without performing a RCA, the organization may not be able to address the root cause and may face the same or similar incidents in the future, which could result in more damage, costs, and reputational loss. Therefore, the information security manager should prioritize the RCA over other concerns, such as meeting the SLA, RTO, or notification requirements, which are important but secondary to the RCA.
References = CISM Review Manual 15th Edition, page 254-2551; CISM Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 4202

NEW QUESTION: 302
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:
A. service level agreements (SLAs)
B. security requirements for the process being outsourced.
C. risk-reporting methodologies.
D. security metrics
Answer: (SHOW ANSWER)
Explanation
An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus primarily on defining security requirements for the process being outsourced.
Security requirements are the specifications of what needs to be done to protect the information assets from unauthorized access, use, disclosure, modification, or destruction. Security requirements should be aligned with the organization's risk appetite and business objectives, and should cover both technical and organizational aspects of the service delivery. Security requirements should also be clear, concise, measurable, achievable, realistic, and testable. References = CISM Review Manual (Digital Version), Chapter 3:
Information Security Risk Management, Section 3.1: Risk Identification, p. 115-1161. CISM Review Manual (Print Version), Chapter 3: Information Security Risk Management, Section 3.1: Risk Identification, p.

115-1162. CISM ITEM DEVELOPMENT GUIDE, Domain 3: Information Security Program Development and Management, Task Statement 3.1, p. 193.
Security requirements for the process being outsourced are the specifications and standards that the third party must comply with to ensure the confidentiality, integrity and availability of the critical business information.
They define the roles and responsi-bilities of both parties, the security controls and measures to be implemented, the se-curity objectives and expectations, the security risks and mitigation strategies, and the security monitoring and reporting mechanisms. Security requirements are essential to protect the information assets of the organization and to establish a clear and en-forceable contractual relationship with the third party.
References:
*1 Outsourcing Strategies for Information Security: Correlated Losses and Security Exter-nalities - SpringerLink
*2 What requirements must outsourcing services comply with for the European market? - CBI
*3 Outsourcing cybersecurity: What services to outsource, what to keep in house - Infosec Institute
*4 BCFSA outsourcing and information security guidelines - BLG

NEW QUESTION: 303
Which of the following is the BEST tool to monitor the effectiveness of information security governance?
A. Key performance indicators (KPIs)
B. Balanced scorecard
C. Business impact analysis (BIA)
D. Risk profile
Answer: (SHOW ANSWER)
Explanation
Key performance indicators (KPIs) are the best tool to monitor the effectiveness of information security governance because they are quantifiable and measurable metrics that reflect the achievement of the information security objectives and the alignment of the information security strategy with the business goals. KPIs can help to evaluate the performance, efficiency, quality, and value of the information security processes and activities, and to identify the areas of improvement or adjustment. KPIs can also provide feedback to the management and the stakeholders on the status and progress of the information security governance. Some examples of KPIs for information security governance are: percentage of compliance with security policies and standards, number and severity of security incidents, return on security investment, and maturity level of information security capabilities12.
A balanced scorecard is a strategic management tool that translates the vision and mission of the organization into four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help to align the information security strategy with the business strategy, but it is not a tool to monitor the effectiveness of information security governance. A balanced scorecard can include KPIs as part of its measurement system, but it is not a substitute for KPIs13.
A business impact analysis (BIA) is a process of assessing the potential consequences of a disruption to the organization's critical business functions or processes. A BIA can help to identify the critical assets, dependencies, recovery priorities, and recovery objectives for the information security program, but it is not a

tool to monitor the effectiveness of information security governance. A BIA is a one-time or periodic activity, not a continuous monitoring process14.
A risk profile is a representation of the organization's exposure to various types of risks, such as operational, financial, strategic, or reputational. A risk profile can help to identify the sources, likelihood, and impact of potential threats to the organization's assets and objectives, and to determine the risk appetite and tolerance for the information security program, but it is not a tool to monitor the effectiveness of information security governance. A risk profile is a snapshot of the organization's risk posture at a given point in time, not a dynamic monitoring tool15. References = CISM Review Manual, 16th Edition, pages 23-241; CISM Exam Content Outline, Domain 1, Knowledge Statement 1.122; CISM Review Questions, Answers & Explanations Database, Question ID 10093; CISM Review Questions, Answers & Explanations Database, Question ID 10104; CISM Review Questions, Answers & Explanations Database, Question ID 10115

NEW QUESTION: 304
Which of the following is the BEST option to lower the cost to implement application security controls?
A. Perform security tests in the development environment.
B. Integrate security activities within the development process
C. Perform a risk analysis after project completion.
D. Include standard application security requirements
Answer: (SHOW ANSWER)
Explanation
Integrating security activities within the development process is the best option to lower the cost to implement application security controls because it ensures that security is considered and addressed throughout the software development life cycle (SDLC), from design to deployment, and reduces the likelihood and impact of security flaws or vulnerabilities that may require costly fixes or patches later on. Performing security tests in the development environment is not the best option because it may not detect or prevent all security issues that may arise in different environments or scenarios. Performing a risk analysis after project completion is not a good option because it may be too late to identify or mitigate security risks that may have been introduced during the project. Including standard application security requirements is not a good option because it may not account for specific or unique security needs or challenges of different applications or projects.
References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/secure-software-development-lifecycle
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information

NEW QUESTION: 305
Which of the following BEST enables an organization to effectively manage emerging cyber risk?
A. Periodic internal and external audits
B. Clear lines of responsibility
C. Sufficient cyber budget allocation
D. Cybersecurity policies
Answer: (SHOW ANSWER)

Explanation
Cybersecurity policies are the high-level statements that define the organization's objectives, principles, and expectations for protecting its information assets from cyber threats. Cybersecurity policies provide the foundation for developing and implementing cybersecurity strategies, plans, procedures, standards, and guidelines. However, cybersecurity policies alone are not enough to ensure effective cybersecurity. The organization also needs to allocate sufficient budget resources to support the implementation and maintenance of cybersecurity controls, such as hardware, software, personnel, training, testing, auditing, and incident response. Sufficient cyber budget allocation demonstrates the organization's commitment to cybersecurity and enables it to achieve its cybersecurity goals. References: https://www.isaca.org/credentialing/cism https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-978111980194

NEW QUESTION: 306
Which of the following is MOST important for the effective implementation of an information security governance program?
A. Employees receive customized information security training
B. The program budget is approved and monitored by senior management
C. The program goals are communicated and understood by the organization.
D. Information security roles and responsibilities are documented.
Answer: (SHOW ANSWER)
Explanation
The program goals are communicated and understood by the organization is the most important factor for the effective implementation of an information security governance program because it ensures that the program is aligned with the business objectives and supported by the stakeholders. Employees receive customized information security training is not the most important factor, but rather a means to achieve the program goals and raise awareness among the staff. The program budget is approved and monitored by senior management is not the most important factor, but rather a resource to enable the program activities and measure its performance. Information security roles and responsibilities are documented is not the most important factor, but rather a way to define and assign the program tasks and accountabilities. References: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/how-to-measure-the-effectiveness-of-inform
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/how-to-align-security-initiatives-with-busin

NEW QUESTION: 307
Which of the following should an information security manager do FIRST when a vulnerability has been disclosed?
A. Perform a patch update.
B. Conduct a risk assessment.
C. Perform a penetration test.
D. Conduct an impact assessment.
Answer: (SHOW ANSWER)
Explanation

According to the CISM Review Manual, the first step an information security manager should take when a vulnerability has been disclosed is to conduct a risk assessment to determine the likelihood and impact of the vulnerability being exploited, and the appropriate response strategy. Performing a patch update, a penetration test or an impact assessment are possible subsequent steps, but not the first one.
References = CISM Review Manual, 27th Edition, Chapter 3, Section 3.3.2, page 1331.

NEW QUESTION: 308
An information security manager developing an incident response plan MUST ensure it includes:
A. an inventory of critical data.
B. criteria for escalation.
C. a business impact analysis (BIA).
D. critical infrastructure diagrams.
Answer: (SHOW ANSWER)
Explanation
An incident response plan is a set of procedures and guidelines that define the roles and responsibilities of the incident response team, the steps to follow in the event of an incident, and the communication and escalation protocols to ensure timely and effective resolution of incidents. One of the essential components of an incident response plan is the criteria for escalation, which specify the conditions and thresholds that trigger the escalation of an incident to a higher level of authority or a different function within the organization. The criteria for escalation may depend on factors such as the severity, impact, duration, scope, and complexity of the incident, as well as the availability and capability of the incident response team. The criteria for escalation help to ensure that incidents are handled by the appropriate personnel, that management is kept informed and involved, and that the necessary resources and support are provided to resolve the incident. References = https://blog.exigence.io/a-practical-approach-to-incident-management-escalation https://www.uc.edu/content/dam/uc/infosec/docs/Guidelines/Information_Security_Incident_Response_Escalatio

NEW QUESTION: 309
The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:
A.)the information security officer.
B. the steering committee.
C. the board of directors.
D. the internal audit manager.
Answer: (SHOW ANSWER)
Explanation
The ultimate responsibility for ensuring the objectives of an information security framework are being met belongs to the board of directors, as they are accountable for the governance of the organization and the oversight of the information security strategy. The board of directors should ensure that the information security framework aligns with the business objectives, supports the business processes, and complies with the legal and regulatory requirements. The board of directors should also monitor the performance and effectiveness of the information security framework and provide guidance and direction for its improvement.

References = CISM Review Manual, 16th Edition eBook1, Chapter 1: Information Security Governance, Section: Enterprise Governance, Subsection: Board of Directors, Page 18.

NEW QUESTION: 310

Which of the following is the PRIMARY responsibility of the information security function when an organization adopts emerging technologies?

A. Developing security training for the new technologies
B. Designing new security controls
C. Creating an acceptable use policy for the technologies
D. Assessing the potential security risk
Answer: (SHOW ANSWER)
Explanation
The primary responsibility of the information security function when an organization adopts emerging technologies is to assess the potential security risk, which means identifying and evaluating the threats, vulnerabilities, and impacts that the new technologies may pose to the organization's data, systems, and objectives. Assessing the potential security risk helps the information security function to determine the appropriate security requirements, controls, and measures to mitigate the risk and ensure the safe and secure adoption of the emerging technologies.
References = Performing Risk Assessments of Emerging Technologies, CISM Review Manual 15th Edition
Learn more:
1. isaca.org2. isaca.org3. niccs.cisa.gov4. venturebeat.com
10of30
An organization is planning to outsource network management to a service provider. Including which of the following in the contract would be the MOST effective way to mitigate information security risk? A. Requirement for regular information security awareness B. Right-to-audit clause C. Service level agreement (SLA) D. Requirement to comply with corporate security policy answer: (Refer to the Information Security Manager (CISM) documents and learning resources by ISACA available at https://store.isaca.org/s/store#/store/browse/cat/a2D4w00000Ac6NNEAZ/tiles to verify the answer of the following questions very carefully.) Use the following format please: **Verified Answer** = (From CISM Manual or related resources) **Very Short Explanation** = (From CISM Manual or related resources) **References** = (From CISM Manual or related resources) ==========

NEW QUESTION: 311
Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?
A. Requiring an external security audit of the IT service provider
B. Requiring regular reporting from the IT service provider
C. Defining information security requirements with internal IT
D. Defining the business recovery plan with the IT service provider
Answer: (SHOW ANSWER)
Explanation

Requiring regular reporting from the IT service provider is the best way to ensure compliance with the organization's information security requirements, as it allows the organization to monitor the performance, security incidents, service levels, and compliance status of the IT service provider. Reporting also helps to identify any gaps or issues that need to be addressed or resolved. (From CISM Review Manual 15th Edition) References: CISM Review Manual 15th Edition, page 184, section 4.3.3.2.

NEW QUESTION: 312
Which of the following is the MOST important consideration when establishing an organization's information security governance committee?
A. Members have knowledge of information security controls.
B. Members are business risk owners.
C. Members are rotated periodically.
D. Members represent functions across the organization.
Answer: (SHOW ANSWER)
Explanation
= The most important consideration when establishing an organization's information security governance committee is to ensure that members represent functions across the organization. This is because the information security governance committee is responsible for setting the direction, scope, and objectives of the information security program, and for ensuring that the program aligns with the organization's business goals and strategies. By having members from different functions, such as finance, human resources, operations, legal, and IT, the committee can ensure that the information security program considers the needs, expectations, and perspectives of various stakeholders, and that the program supports the organization's mission, vision, and values. Having a diverse and representative committee also helps to foster a culture of security awareness and accountability throughout the organization, and to promote collaboration and communication among different functions.
Members having knowledge of information security controls, members being business risk owners, and members being rotated periodically are all desirable characteristics of an information security governance committee, but they are not the most important consideration. Members having knowledge of information security controls can help the committee to understand the technical aspects of information security and to evaluate the effectiveness and efficiency of the information security program. However, having technical knowledge is not sufficient to ensure that the information security program is aligned with the organization's business goals and strategies, and that the program considers the needs and expectations of various stakeholders. Members being business risk owners can help the committee to identify and prioritize the information security risks that affect the organization's business objectives, and to allocate appropriate resources and responsibilities for managing those risks. However, being a business risk owner does not necessarily imply that the member has a comprehensive and balanced view of the organization's information security needs and expectations, and that the member can represent the interests and perspectives of various functions. Members being rotated periodically can help the committee to maintain its independence and objectivity, and to avoid conflicts of interest or complacency. However, rotating members too frequently can also reduce the continuity and consistency of the information security program, and can affect the committee's ability to monitor and evaluate the performance and progress of the information security program. References

=
ISACA, CISM Review Manual, 16th Edition, 2020, pages 36-37.
ISACA, CISM Review Questions, Answers & Explanations Database, 12th Edition, 2020, question ID 1014.

NEW QUESTION: 313
Which of the following should an information security manager do FIRST upon confirming a privileged user's unauthorized modifications to a security application?
A. Report the risk associated with the policy breach.
B. Enforce the security configuration and require the change to be reverted.
C. Implement compensating controls to address the risk.
D. Implement a privileged access management system.
Answer: (SHOW ANSWER)
Explanation
The first thing that an information security manager should do upon confirming a privileged user's unauthorized modifications to a security application is to enforce the security configuration and require the change to be reverted. This is because the unauthorized modification may have compromised the security of the application and the data it protects, and may have violated the security policies and standards of the organization. By enforcing the security configuration and requiring the change to be reverted, the information security manager can restore the security posture of the application and prevent further unauthorized modifications.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the security configuration of information systems is in compliance with the security policies and standards of the organization" and that "the information security manager should monitor and review the security configuration of information systems on a regular basis and take corrective actions when deviations or violations are detected" (p. 138). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Enforcing the security configuration and requiring the change to be reverted is the correct answer because it is the most immediate and effective action to address the unauthorized modification and to maintain the security of the application" (p. 63). Additionally, the Effective Interactive Privileged Access Review article from the ISACA Journal 2018 states that "any unauthorized changes to the production environment should be reverted back to the original state and the incident should be reported to the appropriate authority" (p. 4)1.

NEW QUESTION: 314
An organization has identified a large volume of old data that appears to be unused. Which of the following should the information security manager do NEXT?
A. Consult the record retention policy.
B. Update the awareness and training program.
C. Implement media sanitization procedures.
D. Consult the backup and recovery policy.
Answer: (SHOW ANSWER)
Explanation

The next thing that the information security manager should do after identifying a large volume of old data that appears to be unused is to consult the record retention policy. The record retention policy is a document that defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes. By consulting the record retention policy, the information security manager can determine if the old data is still required to be stored, archived, or disposed of, and how to do so in a secure and compliant manner.
References: The CISM Review Manual 2023 states that "the information security manager is responsible for ensuring that the data lifecycle management process is in alignment with the organization's record retention policy" and that "the record retention policy defines the types, formats, and retention periods of data that the organization needs to keep for legal, regulatory, operational, or historical purposes" (p. 140). The CISM Review Questions, Answers & Explanations Manual 2023 also provides the following rationale for this answer: "Consult the record retention policy is the correct answer because it is the next logical step to take after identifying a large volume of old data that appears to be unused, as it will help the information security manager to decide on the appropriate data lifecycle management actions for the old data, such as storage, archiving, or disposal" (p. 64). Additionally, the article Data Retention Policy: What It Is and How to Create One from the ISACA Journal 2019 states that "a data retention policy is a document that outlines the types, formats, and retention periods of data that an organization needs to keep for various purposes, such as legal compliance, business operations, or historical records" and that "a data retention policy can help an organization to manage its data lifecycle, optimize its storage capacity, reduce its costs, and enhance its security and privacy" (p. 1)1.

NEW QUESTION: 315
An information security manager determines there are a significant number of exceptions to a newly released industry-required security standard. Which of the following should be done NEXT?
A. Document risk acceptances.
B. Revise the organization's security policy.
C. Assess the consequences of noncompliance.
D. Conduct an information security audit.
Answer: (SHOW ANSWER)
Explanation
Assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard. The information security manager should evaluate the potential impact and exposure of the organization due to the noncompliance with the security standard. The assessment should consider the legal, regulatory, contractual, and reputational implications of the noncompliance, as well as the likelihood and severity of the incidents or penalties that may result from the noncompliance. The assessment should also compare the cost and benefit of complying with the security standard versus accepting the risk of noncompliance. The assessment should provide the basis for making informed and rational decisions about how to address the noncompliance issue and prioritize the actions and resources needed to achieve compliance. Documenting risk acceptances, revising the organization's security policy, and conducting an information security audit are all possible actions that may be taken to address the noncompliance issue, but they are not the next steps that should be done.

These actions should be performed after assessing the consequences of noncompliance, and based on the results and recommendations of the assessment. Documenting risk acceptances may be appropriate if the organization decides to accept the risk of noncompliance, and if the risk is within the risk appetite and tolerance of the organization. Revising the organization's security policy may be necessary if the organization decides to comply with the security standard, and if the policy needs to be updated to reflect the new requirements and expectations. Conducting an information security audit may be useful if the organization wants to verify the level of compliance and identify the gaps and weaknesses in the security controls and processes. Therefore, assessing the consequences of noncompliance is the next step that should be done after determining that there are a significant number of exceptions to a newly released industry-required security standard, as it helps the information security manager to understand the risk and impact of the noncompliance and to make informed and rational decisions about how to address it. References = CISM Review Manual 2023, page 43 1; CISM Practice Quiz 2

NEW QUESTION: 316
Which of the following would be the GREATEST threat posed by a distributed denial of service (DDoS) attack on a public-facing web server?
A. Execution of unauthorized commands
B. Prevention of authorized access
C. Defacement of website content
D. Unauthorized access to resources
Answer: (SHOW ANSWER)
Explanation
Prevention of authorized access is the greatest threat posed by a distributed denial of service (DDoS) attack on a public-facing web server because it prevents legitimate users or customers from accessing the web services or resources, causing disruption, dissatisfaction, and potential loss of revenue or reputation. Execution of unauthorized commands is not a threat posed by a DDoS attack, but rather by a remote code execution (RCE) attack. Defacement of website content is not a threat posed by a DDoS attack, but rather by a web application attack. Unauthorized access to resources is not a threat posed by a DDoS attack, but rather by a brute force attack or an authentication bypass attack. References:
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/the-value-of-penetration-testing
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/security-scanning-versus-penetration-testing

NEW QUESTION: 317
An information security manager has become aware that a third-party provider is not in compliance with the statement of work (SOW). Which of the following is the BEST course of action?
A. Notify senior management of the issue.
B. Report the issue to legal personnel.
C. Initiate contract renegotiation.
D. Assess the extent of the issue.
Answer: (SHOW ANSWER)
Explanation
The first course of action when the information security manager becomes aware that a third-party provider is not in compliance with the SOW is to assess the extent of the issue, which means determining the nature, scope, and impact of the non-compliance on the security of the enterprise's data and systems. The assessment should also identify the root cause of the non-compliance and the possible remediation actions. The assessment will help the information security manager to decide the next steps, such as notifying senior management, reporting the issue to legal personnel, initiating contract renegotiation, or terminating the contract.
References = Ensuring Vendor Compliance and Third-Party Risk Mitigation, A Risk-Based Management Approach to Third-Party Data Security, Risk and Compliance

NEW QUESTION: 318
An organization is about to purchase a rival organization. The PRIMARY reason for performing information security due diligence prior to making the purchase is to:
A. determine the security exposures.
B. assess the ability to integrate the security department operations.
C. ensure compliance with international standards.
D. evaluate the security policy and standards.
Answer: (SHOW ANSWER)
Explanation
Information security due diligence is the process of assessing the current state of information security in an organization, identifying any gaps, risks, or vulnerabilities, and estimating the costs and efforts required to remediate them. Performing information security due diligence prior to making the purchase is important to determine the security exposures that may affect the value, reputation, or liability of the organization, as well as the feasibility and compatibility of integrating the security systems and processes of the two organizations.
References = CISM Review Manual 2022, page 361; CISM Exam Content Outline, Domain 1, Task 1.22; Information Security Due Diligence Questionnair

NEW QUESTION: 319
Which of the following risk scenarios is MOST likely to emerge from a supply chain attack?
A. Compromise of critical assets via third-party resources
B. Unavailability of services provided by a supplier
C. Loss of customers due to unavailability of products

D. Unreliable delivery of hardware and software resources by a supplier

Answer: (SHOW ANSWER)

Explanation

= A supply chain attack is a type of cyberattack that targets the suppliers or service providers of an organization, rather than the organization itself. The attackers exploit the vulnerabilities or weaknesses in the supply chain to gain access to the organization's network, systems, or data. The attackers may then use the compromised third-party resources to launch further attacks, steal sensitive information, disrupt operations, or damage reputation. Therefore, the most likely risk scenario that emerges from a supply chain attack is the compromise of critical assets via third-party resources. This scenario poses a high threat to the confidentiality, integrity, and availability of the organization's assets, as well as its compliance and trustworthiness. Unavailability of services provided by a supplier, loss of customers due to unavailability of products, and unreliable delivery of hardware and software resources by a supplier are all possible consequences of a supply chain attack, but they are not the most likely risk scenarios. These scenarios may affect the organization's productivity, profitability, and customer satisfaction, but they do not directly compromise the organization's critical assets. Moreover, these scenarios may be caused by other factors besides a supply chain attack, such as natural disasters, human errors, or market fluctuations. References = CISM Review Manual 2023, page 189 1; CISM Practice Quiz 2

NEW QUESTION: 320

Which of the following should have the MOST influence on an organization's response to a new industry regulation?

A. The organization's control objectives

B. The organization's risk management framework

C. The organization's risk appetite

D. The organization's risk control baselines

Answer: (SHOW ANSWER)

Explanation

The most influential factor on an organization's response to a new industry regulation is the organization's risk appetite. This is because the risk appetite defines the level of risk that the organization is willing to accept in pursuit of its objectives, and it guides the decision-making process for managing risks. The risk appetite also determines the extent to which the organization needs to comply with the new regulation, and the resources and actions required to achieve compliance. The risk appetite should be aligned with the organization's strategy, culture, and values, and it should be communicated and monitored throughout the organization.

NEW QUESTION: 321

A security incident has been reported within an organization When should an information security manager contact the information owner?

A. After the incident has been mitigated

B. After the incident has been confirmed.

C. After the potential incident has been togged

D. After the incident has been contained

Answer: (SHOW ANSWER)

Explanation

= An information security manager should contact the information owner after the incident has been confirmed, as this is the point when the impact and severity of the incident can be assessed and communicated.

The information owner is responsible for the business value and use of the information and should be involved in the decision making process regarding the incident response. Contacting the information owner after the incident has been mitigated or contained may be too late, as the information owner may have different priorities or expectations than the security team. Contacting the information owner after the potential incident has been logged may be premature, as the incident may turn out to be a false positive or a minor issue that does not require the information owner's attention. References = 1: CISM Review Manual, 16th Edition by Isaca (Author), page 292.

NEW QUESTION: 322

A recent application security assessment identified a number of low- and medium-level vulnerabilities. Which of the following stakeholders is responsible for deciding the appropriate risk treatment option?

A. Security manager

B. Chief information security officer (CISO)

C. System administrator

D. Business owner

Answer: (SHOW ANSWER)

Explanation

Verified answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3, "The appropriate risk treatment option is decided by the chief information security officer (CISO) or the designated risk owner."1 Comprehensive and Detailed Explanation: The CISO is the senior executive who is responsible for overseeing and managing the information security program of an organization. The CISO has the authority and expertise to assess the risks, determine the risk appetite and tolerance levels, and select the most suitable risk treatment options for each risk. The CISO also has the accountability and responsibility for implementing, monitoring, and reporting on the risk treatment activities.

References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3

NEW QUESTION: 323

Which of the following is a PRIMARY responsibility of the information security goxernance function?

A. Administering information security awareness training

B. Defining security strategies to support organizational programs

C. Ensuring adequate support for solutions using emerging technologies

D. Advising senior management on optimal levels of risk appetite and tolerance

Answer: B (LEAVE A REPLY)

Explanation

Defining security strategies to support organizational programs is a primary responsibility of the information security governance function, as it involves providing strategic direction for security activities and ensuring that objectives are achieved. According to ISACA, information security governance is a subset of corporate

governance that provides guidance for aligning information security with business objectives, managing information security risks, and using information resources responsibly12.
References = CISM Review Manual, 27th Edition, Chapter 4, Section 4.1.1, page 2131; CISM Online Review Course, Module 4, Lesson 1, Topic 12

NEW QUESTION: 324
An organization is experiencing a sharp increase in incidents related to phishing messages. The root cause is an outdated email filtering system that is no longer supported by the vendor. Which of the following should be the information security manager's FIRST course of action?
A. Reinforce security awareness practices for end users.
B. Temporarily outsource the email system to a cloud provider.
C. Develop a business case to replace the system.
D. Monitor outgoing traffic on the firewall.
Answer: (SHOW ANSWER)
Explanation
Developing a business case to replace the system is the FIRST course of action that the information security manager should take, because it helps to justify the need for a new and effective email filtering system that can prevent or reduce phishing incidents. A business case should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics.
References =
CISM Review Manual, 16th Edition, ISACA, 2020, p. 42: "A business case is a document that provides the rationale and justification for an information security investment. It should include the problem statement, the proposed solution, the costs and benefits, the risks and assumptions, and the expected outcomes and metrics." Email Filtering Explained: What Is It and How Does It Work: "Email filtering is a process used to sort emails and identify unwanted messages such as spam, malware, and phishing attempts. The goal is to ensure that they don't reach the recipient's primary inbox. It is an essential security measure that helps protect users from unwanted or malicious messages." Cloud-based email phishing attack using machine and deep learning ...: "This attack is used to attack your email account and hack sensitive data easily."

NEW QUESTION: 325
Which of the following BEST indicates that information security governance and corporate governance are integrated?
A. The information security team is aware of business goals.
B. The board is regularly informed of information security key performance indicators (KPIs),
C. The information security steering committee is composed of business leaders.
D. A cost-benefit analysis is conducted on all information security initiatives.
Answer: (SHOW ANSWER)
Explanation
The information security steering committee is composed of business leaders is the best indicator that information security governance and corporate governance are integrated, as this shows that the information security program is aligned with the business objectives and strategies, and that the information security

manager has the support and involvement of the senior management. The information security steering committee is responsible for overseeing the information security program, setting the direction and scope, approving policies and standards, allocating resources, and monitoring performance and compliance. The information security steering committee also ensures that the information security risks are communicated and addressed at the board level, and that the information security program is consistent with the corporate governance framework and culture. The information security team is aware of business goals, the board is regularly informed of information security key performance indicators (KPIs), and a cost-benefit analysis is conducted on all information security initiatives are also important, but not as important as the information security steering committee is composed of business leaders, as they do not necessarily imply that the information security governance and corporate governance are integrated, and that the information security program has the authority and accountability to achieve its goals. References = CISM Review Manual 2023, page 271; CISM Review Questions, Answers & Explanations Manual 2023, page 342; ISACA CISM - iSecPrep, page 193

NEW QUESTION: 326

Which of the following would BEST demonstrate the status of an organization's information security program to the board of directors?

A. Information security program metrics

B. Results of a recent external audit

C. The information security operations matrix

D. Changes to information security risks

Answer: (SHOW ANSWER)

Explanation

Information security program metrics are the best way to demonstrate the status of an organization's information security program to the board of directors, as they provide relevant and meaningful information on the performance, effectiveness, and value of the program, as well as the current and emerging risks and the corresponding mitigation strategies. Information security program metrics should be aligned with the business objectives and risk appetite of the organization, and should be presented in a clear and concise manner that enables the board of directors to make informed decisions and provide oversight. (From CISM Review Manual 15th Edition)

References: CISM Review Manual 15th Edition, page 37, section 1.3.2.2.

NEW QUESTION: 327

Which of the following will BEST facilitate the integration of information security governance into enterprise governance?

A. Developing an information security policy based on risk assessments

B. Establishing an information security steering committee

C. Documenting the information security governance framework

D. Implementing an information security awareness program

Answer: (SHOW ANSWER)

Explanation

Establishing an information security steering committee is the best way to facilitate the integration of information security governance into enterprise governance. The information security steering committee is a cross-functional group of senior managers who provide strategic direction, oversight, and support for the information security program. The committee ensures that the information security strategy is aligned with the enterprise strategy, objectives, and risk appetite. The committee also fosters collaboration and communication among various stakeholders and promotes a culture of security awareness and accountability. Developing an information security policy, documenting the information security governance framework, and implementing an information security awareness program are all important activities for implementing and maintaining information security governance, but they do not necessarily facilitate its integration into enterprise governance. These activities may be initiated or endorsed by the information security steering committee, but they are not sufficient to ensure that information security governance is embedded into the enterprise governance structure and processes. References = CISM Review Manual 2023, page 34 1; CISM Practice Quiz 2

NEW QUESTION: 328
Which of the following roles is BEST suited to validate user access requirements during an annual user access review?
A. Access manager
B. IT director
C. System administrator
D. Business owner
Answer: (SHOW ANSWER)
Explanation
The business owner is the best suited role to validate user access requirements during an annual user access review, because the business owner is responsible for determining the business needs and objectives of the users, as well as defining the appropriate access rights and privileges for each user role. The business owner is also accountable for ensuring that the user access is aligned with the organization's policies and standards, and that the user access review is conducted effectively and efficiently1. The access manager, the IT director, and the system administrator are not as suitable as the business owner, because they are more involved in the technical and operational aspects of user access management, rather than the business aspects.
References = Effective User Access Reviews

NEW QUESTION: 329
Which of the following is an example of risk mitigation?
A. Purchasing insurance
B. Discontinuing the activity associated with the risk
C. Improving security controls
D. Performing a cost-benefit analysis
Answer: (SHOW ANSWER)
Explanation

Improving security controls is an example of risk mitigation, which is the process of reducing the likelihood or impact of a risk. Risk mitigation can be achieved by implementing various strategies, such as purchasing insurance, discontinuing the activity associated with the risk, or improving security controls. Purchasing insurance is a form of risk transfer, which is the process of shifting the responsibility or burden of a risk to another party. Discontinuing the activity associated with the risk is a form of risk avoidance, which is the process of eliminating or avoiding a potential source of harm. Performing a cost-benefit analysis is a form of risk evaluation, which is the process of assessing the costs and benefits of different options to manage a risk. References = CISM Review Manual, 16th Edition, page 1741; CISM Review Questions, Answers & Explanations Manual, 10th Edition, page 802