Free Questions for CISM

Shared by Bass on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization has decided to outsource IT operations. Which of the following should be the PRIMARY focus of the information security manager?

Options:

A- Security requirements are included in the vendor contract
B- External security audit results are reviewed.
C- Service level agreements (SLAs) meet operational standards.
D- Business continuity contingency planning is provided

Answer:

A

Explanation:

Security requirements are included in the vendor contract is the primary focus of the information security manager when outsourcing IT operations because it ensures that the vendor is legally bound to comply with the client's security policies and standards, as well as any external regulations or laws. This also helps to define the roles and responsibilities of both parties, the security metrics and controls to be used, and the penalties for non-compliance or breach. Therefore, security requirements are included in the vendor contract is the correct answer.

https://www.techtarget.com/searchsecurity/tip/15-benefits-of-outsourcing-your-cybersecurity-operations

https://www.sciencedirect.com/science/article/pii/S0378720616302166

Question 2

Question Type: MultipleChoice

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

Options:

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:

D

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.

https://www.imperva.com/learn/application-security/penetration-testing/

https://www.netspi.com/blog/technical/web-application-penetration-testing/are-you-testing-your-web-application-for-vulnerabilities/

Question 3

Question Type: MultipleChoice

An investigation of a recent security incident determined that the root cause was negligent handing of incident alerts by system admit manager to address this issue?

Options:

A- Conduct a risk assessment and share the result with senior management.
B- Revise the incident response plan-to align with business processes.
C- Provide incident response training to data custodians.
D- Provide incident response training to data owners.

Answer:

C

Explanation:

The best action for the system admin manager to address the issue of negligent handling of incident alerts by system admins is to provide incident response training to data custodians because it helps to improve their awareness and skills in recognizing and reporting security incidents, and following the incident response procedures and protocols. Conducting a risk assessment and sharing the result with senior management is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Revising the incident response plan to align with business processes is not a good action because it does not address the root cause of the issue or provide any solutions or improvements. Providing incident response training to data owners is not a good action because data owners are not responsible for handling incident alerts or performing incident response tasks. Reference: 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

Question 4

Question Type: MultipleChoice

Which of the following is MOST important in order to obtain senior leadership support when presenting an information security strategy?

Options:

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:

A

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. Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/technical-security-standards-for-information-systems
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/how-to-align-security-initiatives-with-business-goals-and-objectives

Question 5

Question Type: MultipleChoice

An organization is leveraging tablets to replace desktop computers shared by shift-based staff These tablets contain critical business data and are inherently at increased risk of theft Which of the following will BEST help to mitigate this risk''

Options:

A- Deploy mobile device management (MDM)
B- Implement remote wipe capability.
C- Create an acceptable use policy.
D- Conduct a mobile device risk assessment

Answer:

D

Explanation:

A key risk indicator (KRI) is a metric that provides an early warning of potential exposure to a risk. A KRI should be relevant, measurable, timely, and actionable. The most important factor in an organization's selection of a KRI is the criticality of information, which means that the KRI should reflect the value and sensitivity of the information assets that are exposed to the risk. For example, a KRI for data breach risk could be the number of unauthorized access attempts to a database that contains confidential customer data. The criticality of information helps to prioritize the risks and focus on the most significant ones. Reference: https://www.isaca.org/credentialing/cism

https://www.wiley.com/en-us/CISM+Certified+Information+Security+Manager+Study+Guide-p-9781119801948

Question 6

Question Type: MultipleChoice

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

Options:

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:

D

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.

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-media-relations-during-a-critical-incident/

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

ation-plan.

Question 7

Question Type: MultipleChoice

Senior management has expressed concern that the organization's intrusion prevention system (IPS) may repeatedly disrupt business operations Which of the following BEST indicates that the information security manager has tuned the system to address this concern?

Options:

A- Increasing false negatives
B- Decreasing false negatives
C- Decreasing false positives
D- Increasing false positives

Answer:

C

Explanation:

Decreasing false positives is the best indicator that the information security manager has tuned the system to address senior management's concern that the organization's intrusion prevention system (IPS) may repeatedly disrupt business operations. False positives are alerts generated by the IPS when it mistakenly blocks legitimate traffic or activity, causing disruption or downtime. Decreasing false positives means that the IPS has been configured to reduce such errors and minimize unnecessary interruptions. Increasing false negatives is not a good indicator because it means that the IPS has failed to detect or block malicious traffic or activity, increasing the risk of compromise or damage. Decreasing false negatives is not a good indicator because it does not affect business operations, but rather improves security detection or prevention. Increasing false positives is not a good indicator because it means that the IPS has increased its errors and interruptions, worsening senior management's concern. Reference:
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

Question 8

Question Type: MultipleChoice

Which of the following is MOST helpful in determining the criticality of an organization's business functions?

Options:

A- Disaster recovery plan (DRP)
B- Business impact analysis (BIA)
C- Business continuity plan (BCP)
D- Security assessment report (SAR)

Answer:

B

Explanation:

Business impact analysis (BIA) is the most helpful in determining the criticality of an organization's business functions because it is a process of identifying and evaluating the potential effects of disruptions or interruptions to those functions. BIA helps to prioritize the recovery of the most critical functions and to estimate the resources and time needed for the recovery. Therefore, business impact analysis (BIA) is the correct answer.

https://www.linkedin.com/pulse/business-continuity-critical-functions-tino-marquez

https://www.techtarget.com/searchitchannel/feature/Business-impact-analysis-for-business-continuity-Understanding-impact-criticality

Question 9

Question Type: MultipleChoice

Which of the following is MOST important when defining how an information security budget should be allocated?

Options:

A- Regulatory compliance standards
B- Information security strategy
C- Information security policy
D- Business impact assessment

Answer:

B

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.

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.html

https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/