Free Questions for CISM by go4braindumps

Shared by Carrillo on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following BEST supports effective communication during information security incidents7

Options:

A- Frequent incident response training sessions

B- Centralized control monitoring capabilities

C- Responsibilities defined within role descriptions

D- Predetermined service level agreements (SLAs)

Answer:

D

Explanation:

The best way to support effective communication during information security incidents is to have predetermined service level agreements (SLAs) because they define the expectations and responsibilities of the parties involved in the incident response process, and specify the communication channels, methods, and frequency for reporting and updating on the incident status and resolution.

Frequent incident response training sessions are not very effective because they do not address the communication needs or challenges during an actual incident. Centralized control monitoring capabilities are not very effective because they do not address the communication needs or challenges during an actual incident. Responsibilities defined within role descriptions are not very effective because they do not address the communication needs or challenges during an actual incident. 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 2

Question Type: MultipleChoice

Which of the following has the GREATEST influence on the successful integration of information security within the business?

Options:

A- Organizational structure and culture

B- Risk tolerance and organizational objectives

C- The desired state of the organization

D- Information security personnel

Answer:

A

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. 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 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

The MOST important information for influencing management's support of information security is:

Options:

A- an demonstration of alignment with the business strategy.

B- An identification of the overall threat landscape.

C- A report of a successful attack on a competitor.

D- An identification of organizational risks.

Answer:

A

Explanation:

The most important information for influencing management's support of information security is an demonstration of alignment with the business strategy because it shows how information security contributes to the achievement of the organization's goals and objectives, and adds value to the organization's performance and competitiveness. An identification of the overall threat landscape is not very important because it does not indicate how information security addresses or mitigates the threats or risks. A report of a successful attack on a competitor is not very important because it does not indicate how information security prevents or responds to such attacks. An identification of organizational risks is not very important because it does not indicate how information security manages or reduces the risks. 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

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 6

Question Type: MultipleChoice

From an information security perspective, legal issues associated with a transborder flow of technology-related items are MOST often

Options:

A- website transactions and taxation.

B- software patches and corporate date.

C- encryption tools and personal data.

D- lack of competition and free trade.

Answer:

C

Explanation:

Encryption tools and personal data are the most often associated with legal issues in the context of transborder flow of technology-related items because they involve the protection of privacy and security of individuals and organizations across different jurisdictions, and may be subject to different laws and regulations that govern their access, use, or transfer. Website transactions and taxation are not

very often associated with legal issues in this context because they involve the exchange of goods and services and the collection of taxes across different jurisdictions, which may not be directly related to technology transfer or data flow. Software patches and corporate data are not very often associated with legal issues in this context because they involve the maintenance and improvement of software functionality and the management and sharing of business information, which may not be directly related to technology transfer or data flow. Lack of competition and free trade are not very often associated with legal issues in this context because they involve the market structure and trade policies of different jurisdictions, which may not be directly related to technology transfer or data flow. Reference: https://www.oecd-ilibrary.org/science-and-technology/oecd-declaration-on-transborder-data-flows_230240624407 https://legalinstruments.oecd.org/public/doc/108/108.en.pdf

Question 7

Question Type: MultipleChoice

An email digital signature will:

Options:

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:

B

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. Reference: https://support.microsoft.com/en-us/office/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-b3f4b5856fc6 https://www.techtarget.com/searchsecurity/definition/digital-signature

Question 8

Question Type: MultipleChoice

An information security manager has identified that security risks are not being treated in a timely manner. Which of the following

Options:

A- Provide regular updates about the current state of the risks.

B- Re-perform risk analysis at regular intervals.

C- Assign a risk owner to each risk

D- Create mitigating controls to manage the risks.

Answer:

B

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. Reference: https://support.microsoft.com/en-us/office/secure-messages-by-using-a-digital-signature-549ca2f1-a68f-4366-85fa-

b3f4b5856fc6 https://www.techtarget.com/searchsecurity/definition/digital-signature

Question 9

Question Type: MultipleChoice

To ensure that a new application complies with information security policy, the BEST approach is to:

Options:

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:

C

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. Reference: 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