CRISC Domain 3 Risk Response and Mitigation Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. **For a global enterprise subject to multiple governmental regulations, what is the recommended approach?**
   - **A. Conform all locations to the aggregate requirements**
   - **B. Conform to a generally accepted set of industry practices**
   - **C. Establish a baseline standard with common requirements**
   - **D. Establish baseline standards and add specific requirements as necessary**

2. **Which response option is primarily concerned with reducing risk to an acceptable level?**
   - **A. Risk acceptance**
   - **B. Risk avoidance**
   - **C. Risk mitigation**
   - **D. Risk transfer**

3. **Which of the following BEST protects the confidentiality of data being transmitted over a network?**
   - **A. Data re-encapsulated in data packets with authentication headers.**
   - **B. A digital hash is appended to all messages sent over the network.**
   - **C. Network devices are hardened in compliance with corporate standards.**
   - **D. Fiber-optic cables are used instead of copper cables.**

4. **If a procurement employee discovers that new printer models save printed documents, what should they do to mitigate the risk of data disclosure?**
   - **A. Proceed with the order and configure data wiping.**
   - **B. Notify the security manager for a risk assessment.**
   - **C. Seek another vendor that offers safer printers.**
   - **D. Notify staff to wipe data when decommissioning printers.**

5. **Which factor is crucial in determining the necessary response to identified risks?**
   - **A. The cost of implementing controls**
   - **B. The duration of the risk**
   - **C. The reputation of the organization**
   - **D. The history of previous incidents**

6. In which phase of the system development life cycle is it crucial to define the process to amend deliverables?

A. Feasibility.

B. Development.

C. User acceptance.

D. Design.

7. Which of the following internal controls is essential to protect sensitive pricing information?

A. Identification and authentication

B. Authentication and authorization

C. Segregation of duties (SoD) and authorization

D. Availability and confidentiality

8. What is the primary purpose of a risk assessment in the context of policy deviation?

A. To ensure compliance with existing policies

B. To identify stricter policies that need to be added

C. To determine the risks related to policy noncompliance

D. To evaluate if the costs exceed potential losses

9. In which case is 'risk acceptance' the most viable risk response?

A. When the potential loss is significantly high

B. When the cost of prevention exceeds potential losses

C. When transferring risk is not feasible

D. When risk mitigation offers minimal benefits

10. Encryption of stored data is primarily aimed at protecting data against what?

A. Unauthorized access during transmission

B. Physical theft

C. Unauthorized recovery without the encryption key

D. Accidental deletion

Answers

1. D
2. C
3. A
4. B
5. A
6. A
7. B
8. C
9. B
10. C

Explanations

1. For a global enterprise subject to multiple governmental regulations, what is the recommended approach?

A. Conform all locations to the aggregate requirements

B. Conform to a generally accepted set of industry practices

C. Establish a baseline standard with common requirements

D. Establish baseline standards and add specific requirements as necessary

The recommended approach for a global enterprise facing multiple governmental regulations involves establishing baseline standards and adding specific requirements as necessary. This method is effective because it allows the organization to create a foundational framework that addresses the most critical and common regulatory needs across all locations. By starting with a baseline, the enterprise ensures a uniform level of compliance that meets general legal and operational standards. From this foundation, specific local regulations can be layered on, tailored to regional or country-specific requirements. This flexibility is essential in a global context where regulations can vary significantly. It promotes efficiency by avoiding the need to develop entirely unique compliance strategies for each jurisdiction from scratch, thereby saving time and resources. This approach also enhances scalability, ensuring that as new regulations emerge or as the enterprise expands into new regions, the organization can adapt without overhauling its entire compliance strategy. The focus on establishing a baseline standard before addressing specific requirements reflects a strategic risk management practice, allowing for greater oversight and control over compliance efforts throughout the organization.

2. Which response option is primarily concerned with reducing risk to an acceptable level?

A. Risk acceptance

B. Risk avoidance

C. Risk mitigation

D. Risk transfer

The focus of the response option that emphasizes reducing risk to an acceptable level is risk mitigation. This process involves implementing measures or controls that aim to minimize the likelihood of a risk occurring or to lessen its impact if it does happen. Risk mitigation strategies can include various actions such as introducing new processes, employing technology, providing training, and increasing security measures, all designed to bring down the risk levels attributed to threats or vulnerabilities within an organization. In contrast, risk acceptance involves acknowledging the existence of a risk and deciding to bear the consequences if it occurs. This does not actively reduce the risk but rather makes a conscious choice to live with it. Risk avoidance means eliminating the risk entirely by changing plans, processes, or activities to steer clear of risk exposure. Lastly, risk transfer entails shifting the risk to another party, such as through insurance or outsourcing, without inherently reducing the risk itself.

3. Which of the following BEST protects the confidentiality of data being transmitted over a network?

A. Data re-encapsulated in data packets with authentication headers.

B. A digital hash is appended to all messages sent over the network.

C. Network devices are hardened in compliance with corporate standards.

D. Fiber-optic cables are used instead of copper cables.

The option that best protects the confidentiality of data being transmitted over a network is the first choice, which involves data being re-encapsulated in data packets with authentication headers. This method combines encapsulation of the data within secure packets and authentication, ensuring not only that the data remains confidential while being transmitted but also that it has not been altered in transit. In networking, encapsulation typically refers to placing data in a secure format that allows it to be transmitted safely across the network. This often involves encryption, which is crucial for maintaining confidentiality. The authentication headers further strengthen this by verifying the integrity and origin of the data, guarding against interception and potential tampering. This layered approach is essential for safeguarding data confidentiality. Other options focus on different security measures, such as hashing, device hardening, and using fiber-optic cables. While these strategies contribute to overall data security and integrity, they do not specifically address the confidentiality of data in transit to the same extent as the use of encrypted data packets with authentication headers. Hashing, for example, ensures data integrity but does not provide confidentiality since it does not encrypt the data. Device hardening improves security posture, and fiber-optic cables may reduce the risk of interception but do not themselves encrypt the data

4. If a procurement employee discovers that new printer models save printed documents, what should they do to mitigate the risk of data disclosure?

A. Proceed with the order and configure data wiping.

B. Notify the security manager for a risk assessment.

C. Seek another vendor that offers safer printers.

D. Notify staff to wipe data when decommissioning printers.

The most appropriate action in this scenario is to notify the security manager for a risk assessment. This step is vital because it allows for a thorough evaluation of the potential data disclosure risks associated with the new printer models. Engaging the security manager can provide a more informed perspective on the implications of the data-saving feature and how it aligns with the organization's risk management framework and compliance requirements. A risk assessment will consider factors such as the sensitivity of the documents that might be printed, the likelihood of unauthorized access to these saved documents, and potential impacts on the organization in case of data breaches. This collaborative approach ensures that all concerns are addressed systematically, and any necessary controls or mitigative measures can be developed in line with overall security policies. Furthermore, ensuring that security experts evaluate the situation can help in developing a comprehensive risk response strategy, which may include technical controls, policy updates, or training for staff regarding best practices in data handling. This proactive approach is essential for maintaining data privacy and compliance with relevant regulations.

5. Which factor is crucial in determining the necessary response to identified risks?

A. The cost of implementing controls

B. The duration of the risk

C. The reputation of the organization

D. The history of previous incidents

The crucial factor in determining the necessary response to identified risks is the cost of implementing controls. This factor is essential because it directly affects an organization's ability to effectively manage and mitigate risks within its budgetary constraints. When evaluating risk responses, organizations must consider whether the cost of implementing specific controls is justified by the potential impact that the risk could have on the organization if it were to occur. Effective risk management involves a cost-benefit analysis where the organization weighs the expenses associated with the implementation of controls against the potential losses from the risks. As such, the financial implications of various response options often guide decision-making processes, ensuring that resources are allocated efficiently and effectively to mitigate risks. Assessing the financial implications helps organizations prioritize which risks to address first based on available budgets, thus facilitating a more strategic approach to risk management that aligns with the organization's overall objectives. The other factors, while relevant in their own contexts, do not carry the same weight when it comes to assessing the feasibility and practicality of risk responses.

6. In which phase of the system development life cycle is it crucial to define the process to amend deliverables?

A. Feasibility.

B. Development.

C. User acceptance.

D. Design.

In the feasibility phase of the system development life cycle (SDLC), it is essential to define the process for amending deliverables because this phase involves evaluating the project's viability in terms of technical, economic, and operational perspectives. During this phase, project stakeholders assess whether the proposed system aligns with organizational goals and can be realistically implemented within the given constraints. Establishing an amendment process at this stage helps ensure that any necessary changes to the project's deliverables can be handled effectively and efficiently. This process allows for the identification of potential risks early on and promotes a structured approach to managing modifications in response to stakeholder feedback, emerging requirements, or changes in the project's environment. By addressing the amendment process early, organizations can minimize disruptions and ensure that the project remains aligned with its intended objectives throughout the SDLC. In contrast, defining an amendment process becomes less critical in the later phases of development (such as development, user acceptance, and design) because the focus during those stages is more on executing and finalizing deliverables. Addressing the amendment process earlier enhances the overall adaptability of the project.

7. Which of the following internal controls is essential to protect sensitive pricing information?

A. Identification and authentication

B. Authentication and authorization

C. Segregation of duties (SoD) and authorization

D. Availability and confidentiality

The correct answer highlights the importance of both authentication and authorization in safeguarding sensitive pricing information. Authentication involves verifying the identity of users who access specific data systems, ensuring that only individuals with the proper credentials can view or manipulate sensitive information. This step is critical to prevent unauthorized access, which could lead to data breaches or mishandling of sensitive pricing details. Authorization, on the other hand, defines what authenticated users are allowed to do within the system. It establishes permissions related to viewing, editing, or sharing data, ensuring that even if someone gains access, they are limited to their authorized actions. This combination of authentication and authorization creates a robust defense against both insider threats and external attacks, effectively protecting the integrity and confidentiality of sensitive pricing information. Together, these controls ensure that only the right individuals have access to sensitive data and that they can only perform actions aligned with their designated roles, making it a vital internal control for protecting sensitive pricing information.

8. What is the primary purpose of a risk assessment in the context of policy deviation?

A. To ensure compliance with existing policies

B. To identify stricter policies that need to be added

C. To determine the risks related to policy noncompliance

D. To evaluate if the costs exceed potential losses

The primary purpose of a risk assessment in the context of policy deviation is to determine the risks related to policy noncompliance. Conducting a risk assessment allows organizations to analyze the potential consequences and vulnerabilities that arise when established policies are not followed. This understanding is crucial for identifying which areas of the organization may be exposed to risks, such as financial loss, reputational damage, or regulatory penalties. By assessing these risks, organizations can make informed decisions about how to address deviations from policies—either by reinforcing compliance measures, adjusting policies, or implementing risk mitigation strategies. This focus on identifying risks associated with noncompliance also aids in prioritizing resources toward the most critical areas where the organization's exposure is highest, enabling better risk management overall.

9. In which case is 'risk acceptance' the most viable risk response?

A. When the potential loss is significantly high

B. When the cost of prevention exceeds potential losses

C. When transferring risk is not feasible

D. When risk mitigation offers minimal benefits

'Risk acceptance' is best applied when the cost of prevention exceeds the potential losses. This approach assumes that the financial impact of a potential risk is less than the expense or resource allocation required to mitigate or transfer that risk. In such scenarios, organizations may determine that it is more economical to accept the risk and deal with any consequences that arise, rather than investing significantly in attempts to prevent it. This strategy is particularly important in budgeting and resource allocation, as it allows organizations to focus their efforts and resources on areas where they can achieve better risk reduction outcomes. In contexts where the likely losses are manageable or fall within an organization's risk tolerance levels, embracing risk acceptance can be seen as a practical and justifiable decision. The other contexts provided are less suitable for risk acceptance, as they deal with situations where costs or consequences would warrant a different approach, such as risk avoidance or transfer. For example, significantly high potential losses typically demand mitigation strategies rather than acceptance.

10. Encryption of stored data is primarily aimed at protecting data against what?

A. Unauthorized access during transmission

B. Physical theft

C. Unauthorized recovery without the encryption key

D. Accidental deletion

The primary goal of encrypting stored data is to safeguard it from unauthorized recovery without the encryption key. When data is encrypted, it is transformed into a secure format that can only be deciphered using the correct key. This means that even if an unauthorized individual gains access to the physical storage device or system where the data resides, they cannot read or use the information unless they possess the encryption key. This is crucial for maintaining data confidentiality and regulatory compliance, particularly for sensitive information such as personal details, financial records, or proprietary data. While encryption can help mitigate risks related to physical theft by making the data unreadable if stolen, its main emphasis is on preventing unauthorized parties from recovering and interpreting the data. With the encryption key being central to access, it creates a protective barrier that is hard for attackers to bypass, thereby enhancing data security significantly.