
Question: 1

An organization plans to implement a new Software as a Service (SaaS) speech-to-text solution. Which of the following is MOST important to mitigate risk associated with data privacy?

- A. Secure encryption protocols are utilized.
- B. Multi-factor authentication is set up for users.
- C. The solution architecture is approved by IT.
- D. A risk transfer clause is included in the contract

Answer: B

Explanation:

Utilizing secure encryption protocols is the most important factor to mitigate risk associated with data privacy when implementing a new Software as a Service (SaaS) speech-to-text solution, as it ensures that the data is protected from unauthorized access, interception, or modification during the transmission and storage in the cloud. Setting up multi-factor authentication for users, approving the solution architecture by IT, and including a risk transfer clause in the contract are not the most important factors, as they may not address the data privacy issue, but rather the data access, quality, or liability issue, respectively. References = CRISC Review Manual, 7th Edition, page 153.

Question: 2

The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:

- A. rectify errors in results of KRIs.
- B. detect changes in the risk profile.
- C. reduce costs of risk mitigation controls.
- D. continually improve risk assessments.

Answer: B

Explanation:

The primary reason for periodically monitoring key risk indicators (KRIs) is to detect changes in the risk profile of the enterprise. KRIs are metrics that provide information on the level of exposure to a specific risk or a group of risks. By monitoring KRIs, the enterprise can identify any deviations from the expected risk level, and take appropriate actions to adjust the risk response or the risk appetite. Monitoring KRIs also helps to validate the effectiveness of risk mitigation controls and the accuracy of risk assessments. Rectifying errors in results of KRIs, reducing costs of risk mitigation controls, and continually improving risk assessments are possible benefits of monitoring KRIs, but they are not the primary reason. References = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.1.1.2, page 175.

Question: 3

While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially. Which of the following would be the BEST approach for the risk practitioner to take?

- A. Temporarily suspend emergency changes.
- B. Document the control deficiency in the risk register.
- C. Conduct a root cause analysis.
- D. Continue monitoring change management metrics.

Answer: C

Explanation:

According to the CRISC Review Manual, a root cause analysis is a technique that identifies the underlying causes of an event or a problem. It helps to determine the most effective actions to prevent or mitigate the recurrence of the event or problem. A root cause analysis is the best approach for the risk practitioner to take in this scenario, because it will help to understand why the number of emergency changes has increased substantially and what can be done to address the issue. The other options are not the best approaches, because they do not address the underlying causes of the problem. Temporarily suspending emergency changes may disrupt the business operations and create more risks. Documenting the control deficiency in the risk register is a passive action that does not resolve the problem. Continuing monitoring change management metrics is an ongoing activity that does not provide any insight into the problem. References = CRISC Review Manual, 7th Edition, Chapter 3, Section 3.2.4, page 130.

Question: 4

Which of the following is the MOST important consideration for prioritizing risk treatment plans when faced with budget limitations?

- A. Inherent risk and likelihood
- B. Management action plans associated with audit findings
- C. Residual risk relative to appetite and tolerance
- D. Key risk indicator (KRI) trends

Answer: C

E xpl anati on:

When prioritizing risk treatment plans under budget constraints, the focus should be on residual risk relative to appetite and tolerance. This ensures that resources are allocated to risks that exceed the organization's risk appetite, aligning treatment efforts with strategic objectives and minimizing critical exposure.

Question: 5

Which of the following is the MOST important reason to link an effective key control indicator (KCI) to relevant key risk indicators (KRIs)?

- A. To monitor changes in the risk environment
- B. To provide input to management for the adjustment of risk appetite
- C. To monitor the accuracy of threshold levels in metrics
- D. To obtain business buy-in for investment in risk mitigation measures

Answer: A

E xpl anati on:

Key control indicators (KCIs) are metrics that measure how well a specific control is performing in reducing the causes, consequences, or likelihood of a risk¹. Key risk indicators (KRIs) are metrics that measure changes in the risk exposure or the potential impact of a risk². By linking an effective KCI to relevant KRIs, the organization can monitor changes in the risk environment and assess how the control is influencing the risk level³. This can help the organization to:

- Identify emerging or escalating risks and take timely and appropriate actions
- Evaluate the effectiveness and efficiency of the control and make improvements if needed
- Align the control with the risk appetite and tolerance of the organization
- Communicate the risk and control status to stakeholders and regulators

References = Risk and Information Systems Control Study Manual, Chapter 6: Risk Response and Mitigation⁴