Isaca

CRISC Exam

Certified in Risk and Information Systems Control

Exam Latest Version: 50.6

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.directcertify.com/isaca/crisc

Question 1. (Single Select)

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 contact

Correct 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. = CRISC Review Manual, 7th Edition, page 153.

Question 2. (Single Select)

The BEST criteria when selecting a risk response is the:

A: capability to implement the response
B: importance of IT risk within the enterprise
C: effectiveness of risk response options
D: alignment ofresponse to industry standards

Correct Answer: C

Explanation:

The effectiveness of risk response options is the best criteria when selecting a risk response, because it reflects the degree to which the response can reduce the impact or likelihood of the risk, or enhance the benefit or opportunity of the risk. The effectiveness of risk response options can be evaluated by considering factors such as cost, feasibility, timeliness, and alignment with the organization's objectives and risk appetite. The other options are not as good as the effectiveness of risk response options, because they do not measure the outcome or value of the response, but rather focus on the input or process of the response, as explained below:

A . Capability to implement the response is a criteria that considers the availability and adequacy of the resources, skills, and knowledge required to execute the response. While this is an important factor to consider, it does not indicate how well the response can address the risk or achieve the desired result.

B . Importance of IT risk within the enterprise is a criteria that considers the significance and priority of the risk in relation to the organization's strategy, objectives, and operations. Whilethis is an important factor to consider, itdoes not indicate how well the response can address the risk or achieve the desired result.

D . Alignment of response to industry standards is a criteria that considers the compliance and conformity of the response with the best practices, norms, and expectations of the industry or sector. While this is an important factor to consider, it does not indicate how well the response can address the risk or achieve the desired result. = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.2.2, page 40. How to Select Your Risk Responses -Rebel's Guide to Project Management, Risk Response Plan in Project Management: Key Strategies & Tips, Risk Responses - options for managing risk - Stakeholdermap.com

Question 3. (Single Select)

During a risk treatment plan review, a risk practitioner finds the approved risk action plan has not been completed However, there were other risk mitigation actions implemented. Which of the fallowing is the BEST course of action?

A: Review the cost-benefit of mitigating controls
B: Mark the risk status as unresolved within the risk register
C: Verify the sufficiency of mitigating controls with the risk owner
D: Update the risk register with implemented mitigating actions

Correct Answer: C

Explanation:

The best course of action for a risk practitioner who finds that the approved risk action plan has not been completed but other risk mitigation actions have been implemented is to verify the sufficiency of mitigating controls with the risk owner. This is because the risk owner is the person who is accountable for the risk and the risk response strategy, and therefore should be consulted to ensure that the alternative actions are adequate and effective in reducing the risk to an acceptable level. The other options are not the best course of action, although they may also be performed after verifying the sufficiency of mitigating controls with the risk owner. Reviewing the cost-benefit of mitigating controls, marking the risk status as unresolved within the risk register, and updating the risk register with implemented mitigating actions are secondary actions that depend on the outcome of the verification process. = Risk and Information Systems Control Study Manual, 7th Edition, Chapter 4, Section 4.3.2, p. 193.

Question 4. (Single Select)

Which of the following is the BEST risk management approach for the strategic IT planning process?

A: Key performance indicators (KPIs) are established to track IT strategicinitiatives.
B: The IT strategic plan is reviewed by the chief information security officer (CISO) and enterprise risk management (ERM).
C: The IT strategic plan is developed from the organization-wide risk management plan.
D: Risk scenarios associated with IT strategic initiatives are identified and assessed.

Correct Answer: D

Explanation:

Identifying and assessing the risk scenarios associated with IT strategic initiatives is the best risk management approach for the strategic IT planning process, because it helps to understand and evaluate the potential or actual threats or opportunities that may affect the achievement or implementation of the IT strategic initiatives, and to determine the appropriate risk responses and controls. A risk scenario is a hypothetical situation or event that describes the source,

cause, consequence, and impact of a risk. A risk scenario can be positive or negative, depending on whether it represents an opportunity or a threat. An IT strategic initiative is a project or program that supports or enables the IT strategy, which is a plan that defines how IT supports and aligns with the organization's vision, mission, and strategy. The strategic IT planning process is a process of developing, implementing, and monitoring the IT strategy and its associated IT strategic initiatives. Identifying and assessing the risk scenarios is the best risk management approach, as it helps to anticipate and prepare for the potential or actual outcomes of the IT strategic initiatives, and to optimize the risk-reward balance and the value delivery of IT. Establishing key performance indicators (KPIs) to track IT strategic initiatives, reviewing the IT strategic plan by the chief information security officer (CISO) and enterprise risk management (ERM), and developing the IT strategic plan from the organization-wide risk management plan are all possible risk management approaches for the strategic IT planning process, but they are not the best approach, as they do not directly address the identification and assessment of the risk scenarios associated with IT strategic initiatives. = Risk and Information Systems Control Study Manual, Chapter 2, Section 2.1.1, page 37

Question 5. (Single Select)

Which of the following practices BEST mitigates risk related to enterprise-wide ethical decision making in a multi-national organization?

A: Customized regional training on local laws and regulations
B: Policies requiring central reporting of potential procedure exceptions
C: Ongoing awarenesstraining to support a common risk culture
D: Zero-tolerance policies for risk taking by middle-level managers

Correct Answer: C

Explanation:

The best practice to mitigate risk related to enterprise-wide ethical decision making in a multi-national organization is to provide ongoing awareness training to support a common risk culture. A common risk culture is a set of shared values, beliefs, and behaviors that influence how the organization identifies, analyzes, responds to, and monitors risks. Ongoing awareness training can help to promote a common risk culture by educating the employees about the enterprise's risk management objectives, policies, procedures, roles, and responsibilities, as well as the ethical standards and expectations that apply to their work. Ongoing awareness training

can also help to reinforce the benefits of ethical decision making and the consequences of unethical behavior. Customized regional training on local laws and regulations, policies requiring central reporting of potential procedure exceptions, and zero-tolerance policies for risk taking bymiddle-level managers are also useful practices, but they are not as effective as ongoing awareness training to support a common risk culture. = CRISC Review Manual, 6th Edition, ISACA, 2015, page 37.

DirectCertify

Unlock Your Potential, Certify Your Success

Full version is available at link below with affordable price.

https://www.directcertify.com/isaca/crisc

30% Discount Coupon Code: LimitedTime2025