ServiceNow Certified Implementation Specialist – Risk and Compliance (CIS-RC) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Control Failure Factor impacts which score?

- **A. Inherent**
- **B. Residual**
- **C. Total**
- **D. Calculated**

2. What does the term "residual risk" refer to?

- **A. Risk that remains after controls are applied**
- **B. Initial risk before controls are implemented**
- **C. Risk that is fully mitigated**
- **D. Risk identified in a risk assessment**

3. Which action can a Policy Owner perform regarding policies in ServiceNow?

- **A. Approve Policy Signature**
- **B. Retire a Policy**
- **C. Create New Risk Assessments**
- **D. Update Control Objectives**

4. What is a primary benefit of having a centralized risk management framework?

- **A. A. Increased development costs**
- **B. B. Improved communication between stakeholders**
- **C. C. Limited visibility of risks**
- **D. D. Complex reporting requirements**

5. What is a necessary step when creating new policies in ServiceNow?

- **A. Must be sourced from regulatory websites**
- **B. They can be copied from existing documents**
- **C. Imported policies require validation**
- **D. Created manually with available templates**

6. What action must be completed before a policy can be automatically published?

A. Related control objectives are marked active

B. Policy exception is closed

C. Policy is approved by all approvers

D. Policy is approved by one approver

7. In the audit engagement approval process, what occurs if the engagement is approved with no remaining tasks or issues?

A. It moves into the Follow Up state

B. It moves into the Closed state

C. It returns to Fieldwork state

D. It enters the Scope state

8. SLE (quantitative) is equivalent to which qualitative term?

A. Impact

B. Engagement

C. Priority

D. Likelihood

9. Under what condition can a Policy Exception not be approved related to the control objective and its state?

A. If the control objective only has controls in Retired state

B. If the control objective is without controls

C. If the control objective is with controls

D. If the control objective only has controls in Draft or Retired state

10. Who can move a Policy record from Review into the next state?

A. The sys admin

B. The compliance manager

C. Any reviewer

D. The named policy owner

Answers

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

Explanations

1. Control Failure Factor impacts which score?

A. Inherent

B. Residual

C. Total

D. Calculated

Control Failure Factor is an important element in risk management and assessment. It directly affects the overall evaluation of risks within an organization. In this context, the "Calculated" score is the correct answer because it is the outcome that integrates various factors, including the Control Failure Factor. The Calculated score takes into account all the relevant inputs, such as inherent risks, existing controls, and the effectiveness of those controls. When controls fail, this factor indicates how much additional risk remains, thereby influencing the overall risk assessment produced by the Calculated score. Essentially, it helps in quantifying the effectiveness of risk mitigation efforts. In contrast, while Inherent and Residual scores are crucial in risk assessment, they do not reflect the direct adjustments made due to control failure; rather, they represent risks before and after mitigation without detailing the impacts of control effectiveness in the scoring formula. Total score as a concept might imply an aggregation but does not specifically address how individual factors, including Control Failure Factor, modify the calculated risk landscape. Thus, focusing on the Computed or Calculated rating captures the intended interplay between control effectiveness and overall risk assessment.

2. What does the term "residual risk" refer to?

A. Risk that remains after controls are applied

B. Initial risk before controls are implemented

C. Risk that is fully mitigated

D. Risk identified in a risk assessment

Residual risk refers to the amount of risk that remains after all known risks have been identified and controls have been applied to mitigate them. In the context of risk management, it is essential to understand that while various measures can be taken to reduce or eliminate certain risks, it is often impossible to eliminate all risks entirely. For instance, even after implementing security measures, there may still be a likelihood of a data breach, which represents the residual risk. This concept emphasizes the importance of recognizing that while controls can minimize risk, an inherent level of risk will likely persist. Organizations must continuously assess and monitor residual risk to ensure they are aware of their risk exposure and can make informed decisions about risk management strategies. The other options pertain to different aspects of risk management. Initial risk refers to the state of risk prior to any controls, fully mitigated risk implies that the risk no longer exists (which does not contribute to the analysis of residual risk), and risk identified in a risk assessment is simply the process of determining potential risks before controls are applied. Understanding the distinction is crucial for effective risk management and development of appropriate mitigation strategies.

3. Which action can a Policy Owner perform regarding policies in ServiceNow?

A. Approve Policy Signature

B. Retire a Policy

C. Create New Risk Assessments

D. Update Control Objectives

The action that a Policy Owner can perform regarding policies in ServiceNow is retiring a policy. A Policy Owner has the responsibility and authority to manage the lifecycle of policies, which includes the ability to retire them when they are no longer relevant, necessary, or when a new version has been implemented. Retiring a policy ensures that outdated documents no longer create confusion or lead to compliance issues within the organization. The other actions listed, such as approving policy signatures, creating new risk assessments, and updating control objectives, are generally responsibilities assigned to different roles within the ServiceNow framework. For instance, approving policy signatures often involves a governance or compliance role rather than just the policy ownership, while risk assessments and control objectives relate more to risk management functions that may not fall under the direct purview of a Policy Owner. Therefore, retiring a policy is the specific action aligned with the duties typically assigned to a Policy Owner in the context of managing policies in ServiceNow.

4. What is a primary benefit of having a centralized risk management framework?

A. A. Increased development costs

B. B. Improved communication between stakeholders

C. C. Limited visibility of risks

D. D. Complex reporting requirements

Having a centralized risk management framework significantly enhances communication between stakeholders. This benefit arises because a centralized approach ensures that all relevant parties access the same information and data regarding risks. Stakeholders include risk managers, executives, and operational teams who need to collaborate and share insights effectively. When risks are managed in a centralized framework, it fosters a common understanding of risks across various departments. This shared comprehension aids in aligning risk management strategies with organizational goals, enabling informed decision-making and collective prioritization of risk mitigation efforts. Moreover, open communication channels ensure that updates, insights, and evolving risk assessments are disseminated readily, enabling quicker responses to emerging risks. In contrast, options suggesting increased development costs, limited visibility of risks, and complex reporting requirements do not align with the purpose of a centralized framework. The aim is to streamline processes, enhance visibility, and simplify reporting, making the benefits of improved stakeholder communication a crucial and direct outcome of adopting a centralized risk management approach.

5. What is a necessary step when creating new policies in ServiceNow?

A. Must be sourced from regulatory websites

B. They can be copied from existing documents

C. Imported policies require validation

D. Created manually with available templates

When creating new policies in ServiceNow, it is essential to recognize that imported policies require validation. This step is necessary to ensure that the imported content aligns with the organization's requirements and standards, as well as to confirm the accuracy and relevance of the information being used. Validation helps in identifying any inconsistencies, updating outdated references, and facilitating compliance with regulations. This step safeguards the organization from potential risks associated with utilizing outdated or incorrect policy information. It is a critical component in risk management and compliance frameworks, where accuracy and adherence to policies have significant implications for operational integrity and regulatory compliance. Proper validation of imported policies contributes to a robust governance structure that can effectively manage risks. While the other options may have their merits, they do not emphasize the same level of critical importance in the context of ensuring that the policies being adopted are viable, effective, and compliant with the necessary standards.

6. What action must be completed before a policy can be automatically published?

A. Related control objectives are marked active

B. Policy exception is closed

C. Policy is approved by all approvers

D. Policy is approved by one approver

For a policy to be automatically published in ServiceNow's Risk and Compliance module, it is essential that the policy undergoes a formal approval process. Automatic publication signifies that the policy has received the necessary validation within the organization, ensuring that it meets all compliance and governance standards. The requirement for approval by all approvers ensures that any stakeholders or responsible parties have reviewed and consented to the policy, aligning with established organizational procedures for policy management. This comprehensive approach to approval helps maintain integrity and accountability in the organization's compliance practices, fostering trust and clarity among team members and stakeholders. Once all designated approvers give their consent, the policy can be deemed ready for publication. This step is crucial in minimizing potential risks associated with unauthorized or unvetted policies being implemented. In contrast, while marking related control objectives as active, closing policy exceptions, or obtaining approval from just one approver are important steps in the overall policy management process, they do not encompass the entire scope of necessary validations for automatic publication. Only the collective approval from all required approvers solidifies the policy's readiness for release.

7. In the audit engagement approval process, what occurs if the engagement is approved with no remaining tasks or issues?

A. It moves into the Follow Up state

B. It moves into the Closed state

C. It returns to Fieldwork state

D. It enters the Scope state

When an audit engagement is approved with no remaining tasks or issues, it signifies that all requirements and objectives have been successfully met. Consequently, the engagement transitions into the Closed state, marking the formal completion of the audit process. This state indicates that there are no outstanding items or further actions needed, and the engagement can be considered finalized. In this context, moving to the Closed state is a standard procedural step in audit management systems, reflective of a successful conclusion of the engagement. This ensures proper documentation and record-keeping for future reference, allowing stakeholders to understand that all necessary activities related to the audit have been completed and reviewed. The other options do not align with the process of closing an audit engagement. For example, entering the Follow Up state would imply further actions are needed to address outstanding issues, while returning to the Fieldwork state indicates that the preliminary phase of the audit is still ongoing. Entering the Scope state suggests that the engagement is still being defined or is in its initial planning stages, which contradicts the condition of having no remaining tasks or issues. Therefore, the process correctly concludes with the engagement moving into the Closed state.

8. SLE (quantitative) is equivalent to which qualitative term?

A. Impact

B. Engagement

C. Priority

D. Likelihood

SLE, or Single Loss Expectancy, is a quantitative measure used in risk management to estimate the potential financial loss from a single occurrence of a risk event. The qualitative term that is equivalent to SLE is "Impact." Impact refers to the effect or consequence of a risk event on the organization, particularly in terms of financial loss, operational disruption, or reputational damage. When assessing the impact of a potential risk, organizations consider how severe the outcomes could be if that risk materializes. SLE, as a numerical value, gives a concrete representation of this impact by estimating the average loss expected from a single incident. In contrast, terms like engagement, priority, and likelihood do not directly correlate with the quantitative nature of SLE. Engagement typically pertains to involvement and collaboration efforts within risk management processes, priority indicates the importance or urgency of addressing risk based on its significance, and likelihood evaluates the probability of a risk event occurring. While these terms are relevant in the context of risk assessment, they do not reflect the same financial implications as SLE.

9. Under what condition can a Policy Exception not be approved related to the control objective and its state?

A. If the control objective only has controls in Retired state

B. If the control objective is without controls

C. If the control objective is with controls

D. If the control objective only has controls in Draft or Retired state

A Policy Exception cannot be approved if the control objective is without controls because the primary purpose of a control objective is to define the controls that mitigate specific risks. If there are no controls associated with a control objective, there is no framework to evaluate or manage the associated risks, making it impossible to justify any exceptions. In scenarios where control objectives do not have controls, the very basis for establishing risk management policies and procedures is absent. Thus, it is inherently difficult to make a case for an exception, as exceptions are typically granted to accommodate specific circumstances or to address shortcomings in existing controls. Without any controls in place, there can be no rationale for an exception, as there is no existing measure to gauge compliance or effectiveness against which the exception could be evaluated. This situation differentiates itself from other choices where control objectives have at least some controls associated with them, even if they are in states that might limit their effectiveness. In those cases, it may still be possible to approve a policy exception based on the context of the existing controls.

10. Who can move a Policy record from Review into the next state?

A. The sys admin

B. The compliance manager

C. Any reviewer

D. The named policy owner

The named policy owner possesses the authority to move a Policy record from the Review state into the next state. This responsibility aligns with the workflow management in ServiceNow, where specific roles are assigned particular tasks to ensure a streamlined process. The policy owner is typically the individual accountable for that specific policy, and as such, they are entrusted with the decision-making power regarding its progression through the various stages of its lifecycle. In contrast, while other roles such as the system administrator, compliance manager, or any reviewer play important roles in the governance and oversight of policies, they do not have the direct authority to advance the policy without the named owner's input or consent. The system administrator mainly manages the overall system settings, the compliance manager oversees compliance aspects, and reviewers contribute feedback but lack the definitive authority assigned to the policy owner for moving the record forward past the Review stage. This delineation of roles helps to maintain accountability and clarity in policy management processes.