# Certified Governance Risk and Compliance (CGRC) Practice Exam (Sample)

## Study Guide


**Everything you need from our exam experts!**

# Questions

1. **What is the minimum standard process for the certification and accreditation of systems handling U.S. national security information?**

   **A. NIACAP**

   **B. FISMA**

   **C. NIST SP 800-53**

   **D. ISO 27001**

2. **Which process involves implementing risk response plans, monitoring residual risk, and evaluating risk effectiveness throughout a project?**

   **A. Perform Quantitative Risk Analysis**

   **B. Perform Qualitative Risk Analysis**

   **C. Monitor and Control Risks**

   **D. Identify Risks**

3. **What approach should a project manager use to improve project performance through risk analysis with stakeholders?**

   **A. Involve subject matter experts in the risk analysis activities.**

   **B. Focus on the high-priority risks through qualitative risk analysis.**

   **C. Use qualitative risk analysis to quickly assess the probability and impact of risk events.**

   **D. Involve stakeholders only in the phases where the project affects them directly.**

4. **What risk identification approach involves examining the project from four different perspectives?**

   **A. SWOT analysis**

   **B. Root cause analysis**

   **C. Assumptions analysis**

   **D. Influence diagramming techniques**

**5. What is the only output for the qualitative risk analysis process?**

**A. Enterprise environmental factors**

**B. Project management plan**

**C. Risk register updates**

**D. Organizational process assets**

**6. Who is responsible for the review and risk analysis of all contracts regularly?**

**A. The Supplier Manager**

**B. The IT Service Continuity Manager**

**C. The Service Catalogue Manager**

**D. The Configuration Manager**

**7. In risk prioritization, which alternative can Neil provide to Tom regarding project risk sorting?**

**A. Risks may be listed by risk owner**

**B. Risks may be listed by categories**

**C. Risks may be listed based on team input**

**D. Risks may be listed by their technical complexity**

**8. After identifying a new project risk with significant impact but low probability, what should the project manager do first?**

**A. Add the identified risk to a quality control management control chart**

**B. Add the identified risk to the risk register**

**C. Add the identified risk to the issues log**

**D. Add the identified risk to the low-level risk watchlist**

**9. During qualitative risk analysis, which of the following is NOT an indicator of risk priority?**

**A. Symptoms**

**B. Cost of the project**

**C. Warning signs**

**D. Risk rating**

**10. What is the primary function of a System Authorization Plan (SAP)?**

**A. To authorize management systems**

**B. To define assessment protocols**

**C. To guide risk management activities**

**D. To ensure regulatory compliance**

# Answers

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

# Explanations

## 1. What is the minimum standard process for the certification and accreditation of systems handling U.S. national security information?

**A. NIACAP**

**B. FISMA**

**C. NIST SP 800-53**

**D. ISO 27001**

**The minimum standard process for the certification and accreditation of systems handling U.S. national security information is NIACAP, which stands for the National Information Assurance Certification and Accreditation Process. NIACAP is specifically designed to ensure that information systems in the U.S. federal government, particularly those that are involved with national security, are adequately assessed for security risks and accredited to operate within defined security parameters. NIACAP provides a structured approach to evaluating the security posture of systems and ensuring that appropriate controls are in place, making it particularly relevant for systems handling sensitive government information. This process encompasses various phases, such as system identification, certification, and continuous monitoring, which are critical in maintaining the integrity and confidentiality of national security information. While FISMA establishes a framework for federal information security management, and NIST SP 800-53 provides guidelines for selecting and specifying security controls for federal information systems, neither of them serves specifically as the standard process for certification and accreditation of systems dealing with national security. ISO 27001 is a global standard for information security management systems but does not pertain specifically to U.S. national security considerations. Therefore, NIACAP is the most suitable answer in this context.**

## 2. Which process involves implementing risk response plans, monitoring residual risk, and evaluating risk effectiveness throughout a project?

**A. Perform Quantitative Risk Analysis**

**B. Perform Qualitative Risk Analysis**

**C. Monitor and Control Risks**

**D. Identify Risks**

**The process that involves implementing risk response plans, monitoring residual risk, and evaluating risk effectiveness throughout a project is indeed the monitoring and control phase of risk management. This stage is crucial because it ensures that the risk response strategies are actively working as intended and allows the project team to make necessary adjustments if the responses are not effective or if new risks emerge. During this process, project managers will continuously assess the risk environment, track identified risks, and observe any changes that could impact the project's objectives. By monitoring residual risks—those risks that remain after response measures have been applied—the team can ensure that these risks are within acceptable limits and do not derail project success. Additionally, evaluating the effectiveness of risk responses helps in learning from the project's progression, which can benefit future projects. In contrast to other risk management processes: - Quantitative risk analysis focuses on numerical evaluation of risks, such as estimating the probability and impact of risks, rather than on monitoring or controlling them. - Qualitative risk analysis involves ranking risks based on their potential impact and likelihood but does not engage in the ongoing management of risks throughout the project. - Identifying risks is a preliminary step that involves finding and documenting risks, but it does not address the implementation or monitoring aspects of risk response. Thus**

## 3. What approach should a project manager use to improve project performance through risk analysis with stakeholders?

A. Involve subject matter experts in the risk analysis activities.

B. Focus on the high-priority risks through qualitative risk analysis.

C. Use qualitative risk analysis to quickly assess the probability and impact of risk events.

D. Involve stakeholders only in the phases where the project affects them directly.

**Focusing on high-priority risks through qualitative risk analysis is an effective approach for project managers aiming to enhance project performance. This method allows project managers to identify and prioritize risks that pose the greatest threat to project objectives. By concentrating efforts on these significant risks, project managers can allocate resources more efficiently, create targeted risk response strategies, and ensure that potential issues are addressed proactively. Prioritizing high-priority risks helps in streamlining the risk management process; it enables stakeholders to focus their attention on the most impactful risks, facilitating more informed decision-making. This targeted approach also fosters discussions among stakeholders about the implications of these risks and encourages collaborative solutions, further enhancing project performance. In contrast, while involving subject matter experts and conducting qualitative assessments are important, they may not specifically target the most pressing risks if not aligned with a broader prioritization strategy. Similarly, involving stakeholders only in relevant phases may overlook the benefits of comprehensive engagement throughout the project, which can yield insights into risk factors that might not be immediately evident. Therefore, focusing on high-priority risks offers a structured method for continuously improving project performance by directly addressing the areas of greatest concern.**

## 4. What risk identification approach involves examining the project from four different perspectives?

A. SWOT analysis

B. Root cause analysis

C. Assumptions analysis

D. Influence diagramming techniques

**The approach that involves examining a project from four different perspectives is SWOT analysis. This method assesses the Strengths, Weaknesses, Opportunities, and Threats related to a project or organization. By analyzing these four components, teams can identify a comprehensive set of risks and strategic advantages that might affect project outcomes. Strengths and weaknesses focus on internal factors, helping teams to understand what the organization does well and what areas need improvement. Opportunities and threats, on the other hand, look at external factors that could impact the project, such as market trends or competitive pressures. This holistic view enables better risk identification and can inform proactive decision-making in governance, risk management, and compliance efforts. In contrast, root cause analysis focuses specifically on identifying the underlying reasons for specific problems or defects, which does not provide a broad perspective. Assumptions analysis examines assumptions made within project plans but does so in a less structured manner than SWOT. Influence diagramming helps visualize the relationships between variables but does not systematically address the project from multiple dimensions like SWOT does. Therefore, the comprehensive nature of SWOT analysis makes it the correct choice for this question.**

## 5. What is the only output for the qualitative risk analysis process?

**A. Enterprise environmental factors**

**B. Project management plan**

**C. Risk register updates**

**D. Organizational process assets**

**The correct choice is indeed the updates to the risk register. In the qualitative risk analysis process, the primary goal is to evaluate and prioritize risks based on their probability of occurrence and impact on project objectives. This process leads to a better understanding of the risk landscape and assists in making informed decisions regarding risk responses. As risks are identified and analyzed qualitatively, the outcomes, including any changes in risk priority, newly identified risks, or the reassessed status of existing risks, are documented in the risk register. This register serves as a living document that reflects the current state of risks throughout the project's lifecycle. It is crucial for capturing not only the existing risks but also any updates that arise from the analysis, which helps ensure that stakeholders are aware of the risks facing the project and can respond appropriately. In this context, while enterprise environmental factors, the project management plan, and organizational process assets can influence the risk analysis process, they are not outputs of the qualitative risk analysis itself. They provide essential background and context but do not constitute the direct result of this particular analytical phase. Therefore, the updates made to the risk register are the only definitive output from the qualitative risk analysis process.**

## 6. Who is responsible for the review and risk analysis of all contracts regularly?

**A. The Supplier Manager**

**B. The IT Service Continuity Manager**

**C. The Service Catalogue Manager**

**D. The Configuration Manager**

**The Supplier Manager is typically responsible for the review and risk analysis of all contracts on a regular basis. This role entails managing relationships with suppliers and ensuring that contracts align with the organization’s strategic objectives and compliance requirements. The Supplier Manager assesses the risks associated with supplier engagements, including financial stability, compliance with regulatory frameworks, and alignment with service level agreements. This ongoing analysis is crucial for maintaining effective supplier partnerships and mitigating any potential risks that could impact the organization. In contrast, the other roles relate to different functions within the organization. The IT Service Continuity Manager focuses on ensuring that IT services can continue in the event of disruptions, which involves planning and recovery strategies rather than contract management. The Service Catalogue Manager is responsible for maintaining the service catalogue, ensuring that services offered by the organization are accurately documented and communicated, but this doesn't involve contract reviews. The Configuration Manager manages the configuration items in the IT environment and ensures that they align with IT services, but their responsibilities do not encompass reviewing contracts regularly.**

## 7. In risk prioritization, which alternative can Neil provide to Tom regarding project risk sorting?

**A. Risks may be listed by risk owner**

**B. Risks may be listed by categories**

**C. Risks may be listed based on team input**

**D. Risks may be listed by their technical complexity**

**Listing risks by categories is a strong approach to risk prioritization because it allows for a structured analysis by grouping similar risks together based on shared characteristics or impacts. By categorizing risks, Tom can more easily identify trends, patterns, and vulnerabilities specific to each category, facilitating targeted strategies for mitigation and response. This holistic view can enhance the understanding of how various risks interact and contribute to the overall risk landscape of the project. Furthermore, organizing risks in this manner can aid in efficient resource allocation and management efforts since priorities can be established not just on individual risks but also on the significance of entire categories. This can be particularly beneficial in large-scale projects with numerous risks, as it provides a clearer framework for discussion and decision-making among stakeholders. Options that involve listing by risk owner, team input, or technical complexity might not provide the same level of clarity or actionable insight across a diverse range of risks. While those are certainly useful perspectives for different contexts, categorization stands out as a robust method for effective prioritization in risk management.**

## 8. After identifying a new project risk with significant impact but low probability, what should the project manager do first?

**A. Add the identified risk to a quality control management control chart**

**B. Add the identified risk to the risk register**

**C. Add the identified risk to the issues log**

**D. Add the identified risk to the low-level risk watchlist**

**The best course of action when a project manager identifies a new project risk with significant impact but low probability is to add the identified risk to the risk register. The risk register is a fundamental tool in project management that serves to formally document all identified risks, their characteristics, and their potential impact on the project. By logging this risk in the register, the project manager ensures that it is recognized by the project team and provides a basis for ongoing monitoring and potential mitigation strategies. Maintaining an updated risk register helps the project manager in tracking the risk's status over time and facilitates communication regarding the risk among stakeholders. It also assists in the prioritization of risks for response planning and review during project meetings. Additionally, it demonstrates due diligence and proactive risk management practices within the project. While the other options may seem relevant—such as logging risks in quality control charts, issues logs, or watchlists—these actions do not provide the structured and comprehensive approach that a risk register offers. The quality control management control chart typically deals with defects and quality issues, the issues log focuses on current problems needing resolution rather than potential future risks, and a watchlist may not capture the same level of detail necessary for effective risk management. Thus, placing the risk in the risk register is**

## 9. During qualitative risk analysis, which of the following is NOT an indicator of risk priority?

**A. Symptoms**

**B. Cost of the project**

**C. Warning signs**

**D. Risk rating**

**In qualitative risk analysis, indicators of risk priority are typically related to the potential impact and likelihood of risks affecting a project. Symptoms, warning signs, and risk ratings relate directly to the identification and assessment of risks. Symptoms and warning signs act as early indicators that could point to existing issues or areas of concern, helping teams to prioritize their responses. Risk ratings are a systematic way to quantify risks based on their assessed severity and probability, allowing for effective prioritization. The cost of the project, while certainly an important factor in overall project management and in quantitative assessments, does not serve as a direct indicator of individual risk priority in qualitative analysis. Instead, it is more of a contextual factor that could influence the overall risk management strategy but does not directly correlate to assessing or prioritizing specific risks. Thus, the reference to the cost of the project as an indicator of risk priority in a qualitative analysis context is not applicable.**

## 10. What is the primary function of a System Authorization Plan (SAP)?

**A. To authorize management systems**

**B. To define assessment protocols**

**C. To guide risk management activities**

**D. To ensure regulatory compliance**

**The primary function of a System Authorization Plan (SAP) is to guide risk management activities. A SAP outlines the framework and processes necessary for assessing and managing the risks associated with information systems. It serves as a structured approach to identifying potential security risks, determining their impact on the system and organization, and implementing appropriate controls to mitigate those risks. By focusing on risk management, a SAP ensures that all potential threats are systematically evaluated and addressed, leading to a more secure and compliant system. While options related to authorizing systems, defining assessment protocols, and ensuring compliance are important aspects of governance, they fall under the broader umbrella of risk management. A SAP specifically centers around the identification and management of risks to ensure that systems are authorized based on a thorough assessment of potential vulnerabilities and their implications for the organization. This focus integrates risk management with system authorization processes, making it a critical component of effective governance and compliance practices.**