IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **8020**

Title : ORM Certificate - 2023 Update

Version : DEMO

1.What are the roles of business versus risk management in developing and implementing risk assessments?
A. Risk management, in its role as second line of defense, performs the risk assessment process from beginning to end. There is no business line involvement.
B. The business owns the risk assessment process, while risk management develops the framework, helps facilitate the process, and provides supervision and oversight.
C. Business owns the risk assessment process so risk management does not play a role in the process.
D. Business management's role in the risk assessment process should be confined to oversight.
Answer: B
Explanation:
The Principles for Risk Governance, as established by PRMIA (Professional Risk Managers' International Association), emphasize the Three Lines of Defense (3LoD) Model, which is widely used in risk management and governance frameworks.
Business Line Ownership of Risk (First Line of Defense)
The business units are responsible for identifying, assessing, managing, and monitoring risks within their operations.
Since they generate the risks through their activities, they must own the risk assessment process. This aligns with PRMIA Governance Principles, which state that risk management should be embedded within business operations to ensure proactive risk identification and control. Risk Management’s Role (Second Line of Defense)
The risk management function is not directly responsible for conducting risk assessments but plays a key role in designing and maintaining the risk assessment framework.
This includes setting standards, methodologies, and tools for assessing risks across business functions.
Risk management provides supervision and oversight, ensuring that risk assessments align with organizational policies and regulatory expectations.
Oversight from Senior Management & the Board (Third Line of Defense)
Internal audit (third line of defense) independently reviews and provides assurance that the risk management framework is effective and that risk assessments are conducted properly.
PRMIA’s Risk Governance Standards emphasize that internal audit should evaluate the effectiveness of the risk assessment framework without being involved in its direct execution.
Why Other Answers Are Incorrect
PRMIA Reference for Verification
PRMIA Standards for Risk Governance – Establishes the Three Lines of Defense and the separation of responsibilities.
PRMIA Risk Management Framework (RMF) Guidelines – Defines the roles of business and risk management in risk assessment.
PRMIA Enterprise Risk Management Best Practices – Outlines how risk management facilitates risk assessments while the business retains ownership.
This answer is verified according to PRMIA’s official risk governance documents and best practices.
Would you like additional clarification or supporting documentation references?

2.When a control is found to be ineffective, which of the following steps should be take next?
A. Risks should be re-assessed to determine if there is the appropriate level of control assessment.
B. An action plan should be designed to close the gap.

C. The controls should be re-assessed during the next cycle to determine if they are still ineffective.
D. Risks should be re-assessed to determine if there can be an exception for the level of control assessment.
Answer: B
Explanation:
When a control is found to be ineffective, the primary objective is to remediate the deficiency by implementing corrective measures. PRMIA (Professional Risk Managers' International Association) guidance, aligned with best practices in risk governance, emphasizes a structured approach to handling control deficiencies. Below is a detailed breakdown based on PRMIA risk management principles:
Step 1: Identify and Assess the Ineffective Control
A control is deemed ineffective when it fails to mitigate the identified risks to an acceptable level. The root cause of the failure must be determined through a Control Effectiveness Review (CER). PRMIA recommends control testing and incident analysis to assess the severity of the control failure. Step 2: Develop an Action Plan to Address the Control Deficiency
PRMIA best practices state that risk management should prioritize corrective actions rather than delaying remediation.
The organization must define an action plan to close the gap, which includes:
Revising or strengthening the control mechanisms.
Implementing new controls, if necessary.
Assigning responsibility for remediation to control owners.
Setting deadlines for resolution.
This step aligns with PRMIA's Risk Governance Framework, which emphasizes proactive risk management.
Step 3: Implement Corrective Measures and Monitor Progress
Once an action plan is designed, the organization should execute the corrective actions.
PRMIA's Risk Monitoring Guidelines require regular follow-ups and testing to ensure the control is functioning correctly.
The effectiveness of the remediation should be validated through post-implementation review and ongoing control testing.
Step 4: Re-Assess Risks and Control Effectiveness
Once corrective measures are in place, the organization should re-evaluate risks to confirm that the issue is resolved.
The risk assessment process should be updated to reflect the changes in the control environment.
Why the Other Options Are Incorrect?
Option A: "Risks should be re-assessed to determine if there is the appropriate level of control assessment."
While risk re-assessment is a good practice, it does not directly address the ineffective control.
PRMIA guidelines prioritize closing the control gap first before reassessing risks.
Option C: "The controls should be re-assessed during the next cycle to determine if they are still ineffective."
Waiting until the next assessment cycle delays remediation, which could expose the organization to unmitigated risks.
PRMIA risk frameworks recommend immediate corrective action when a control is found to be ineffective.

Option D: "Risks should be re-assessed to determine if there can be an exception for the level of control assessment."
PRMIA does not support exceptions for ineffective controls unless there is a well-documented risk acceptance process.
A control failure should be remediated rather than seeking exceptions.
PRMIA Risk Reference Used:
PRMIA Risk Governance Framework – Defines the importance of immediate corrective actions for control failures.
PRMIA Risk Monitoring Guidelines – Stresses continuous monitoring and validation of controls.
PRMIA Risk Management Standards – Recommends a structured action plan for ineffective controls.
PRMIA Operational Risk Framework – Emphasizes the need to close control gaps to maintain a strong risk posture.
Final Conclusion:
According to PRMIA risk management best practices, when a control is found to be ineffective, the best course of action is to design and implement an action plan to remediate the issue (Option B). This approach ensures that the organization mitigates risk promptly and maintains a strong control environment.

3.How can a chief risk officer encourage the governing body and executive management team to create a stronger risk culture?
A. Having a vision of achievable but not excessive ambition.
B. Discourage personal accountability to avoid a blame culture.
C. Establish a set of objectives that the board and executive team must adhere to.
D. Balance rewarding success in profitability goals with punishment when there is a failure to achieve goals.
Answer: A
Explanation:
A Chief Risk Officer (CRO) plays a crucial role in shaping and strengthening the risk culture within an organization. PRMIA defines risk culture as the shared values, beliefs, knowledge, and understanding about risk that drive behaviors within an institution. Setting a Clear Vision
The CRO should communicate a vision of risk management that aligns with organizational goals while ensuring that risk-taking remains within acceptable limits.
The vision should be achievable and realistic, rather than overly ambitious, which could incentivize reckless risk-taking.
Embedding Risk Awareness into Decision-Making
A strong risk culture ensures that risk considerations are embedded into business decision-making rather than treated as a separate compliance exercise.
This is supported by PRMIA's Enterprise Risk Management (ERM) Framework, which stresses integrating risk management into strategy and operations. Avoiding a Blame Culture
A risk-aware organization promotes accountability without fear, enabling employees to report risks without retribution.
Option B (Discourage personal accountability to avoid a blame culture) is incorrect because personal accountability is essential for a healthy risk culture. Avoiding a Strict, Prescriptive Approach
A set of rigid objectives that must be followed by the executive team (Option C) does not foster a

dynamic, evolving risk culture.
Instead, risk culture should be flexible and adaptive to emerging risks.
Balancing Incentives and Consequences
While balancing rewards with penalties (Option D) is part of governance, a strong risk culture is not
Incorrect – Reporting, recording, and analysis are correct, but they should not be included in capital calculations.
Explanation
Incorrect – Near misses and opportunity costs provide valuable insights into operational risk, so they should never be ignored. Incorrect – While they should be recorded and analyzed, they are not included in Operational Risk Capital calculations because they do not result in actual losses.
built solely through fear of punishment.
PRMIA emphasizes positive reinforcement, such as linking risk management behaviors to performance evaluations and incentives.
PRMIA Reference for Verification
PRMIA Risk Governance Framework – Discusses the role of leadership in shaping risk culture. PRMIA Standards on Enterprise Risk Management (ERM) – Covers best practices for embedding risk culture within organizations.

4.How should Near Misses and Opportunity Costs be treated within Operational Risk?
A. Ignored.
B. Recorded and Analyzed. Used in calculation of Operational Risk Capital.
C. Reported. Recorded and Analyzed. Not Used in calculation of Operational Risk Capital.
D. Reported, Recorded and Analyzed, Used in calculation of Operational Risk Capital.
Answer: C
Explanation:
Near Misses in Operational Risk
A near miss is an event that could have led to a loss but was avoided or mitigated before actual financial impact occurred.
PRMIA emphasizes that near misses should be reported, recorded, and analyzed because they provide valuable insights into potential vulnerabilities in risk controls.
However, since they did not result in actual financial losses, they are not included in the calculation of Operational Risk Capital.
Opportunity Costs in Operational Risk
Opportunity costs refer to the loss of potential gains due to missed strategic opportunities.
These are not directly quantifiable as operational risk losses and are not included in Operational Risk Capital calculations.
PRMIA's Operational Risk Framework states that operational risk is about actual losses rather than theoretical costs.
Why Other Answers Are Incorrect Option
A. Ignored.
B. Recorded and Analyzed. Used in calculation of Operational Risk Capital.
D. Reported, Recorded, and Analyzed,
Used in calculation of Operational Risk
Capital.

PRMIA Reference for Verification
C. Onsite visits are not advantageous for understanding the third party's risks and control environment.
Why Other Answers Are Incorrect Option
B. An assessment of a third party should not include its compliance and risk infrastructure, financials, business strategy, and operating history.
PRMIA Operational Risk Management Standards – Defines near misses and opportunity costs. Basel II & III Operational Risk Framework – Outlines the principles of operational risk capital calculations.

5.Ideally, which of the following should be completed as part of the risk assessments of service providers?
A. An assessment of a third party should include its compliance and risk infrastructure, financials, business strategy and operating history.
B. An assessment of a third party should not include its compliance and risk infrastructure, financials, business strategy and operating history.
C. Onsite visits are not advantageous for understanding the third party's risks and control environment.
D. A review of the pay levels of the staff supporting the service.
Answer: A
Explanation:
Third-Party Risk Management (TPRM)
PRMIA highlights the importance of conducting thorough due diligence on third-party vendors and service providers.
This includes evaluating compliance programs, risk management frameworks, financial stability, strategic objectives, and operational history.
Key Areas of Third-Party Risk Assessment
Compliance and Risk Infrastructure → Ensures that the provider meets regulatory and security requirements.
Financial Health → Determines whether the provider has the financial stability to support long-term service delivery.
Business Strategy → Helps assess alignment with the organization’s risk appetite and goals.
Operating History → Evaluates experience and reliability in delivering services.
Explanation
Incorrect – Ignoring these critical factors increases the risk of working with an unreliable vendor.
Incorrect – Onsite visits are highly valuable as they provide first-hand insights into operational controls. PRMIA encourages risk managers to conduct site visits.
D. A review of the pay levels of the staff supporting Incorrect – Employee salaries are not a primary risk the service. factor in vendor assessments. The focus should be on the vendor’s security, compliance, and
operational risks.
PRMIA Reference for Verification
PRMIA Third-Party Risk Management (TPRM) Guidelines – Details best practices for vendor risk assessments.
Basel Principles on Outsourcing and Third-Party Risk – Provides regulatory guidance on evaluating third-party service providers.