PRMIA ORM 8020 Practice Questions

Shared by Holt on 29-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the below is accurate about a risk assessment workshop?

Options:

A- The workshop should be run spontaneously so that proper discussion can take place.
B- Although workshops will take on their own form; it is best to prepare thoroughly ahead of time.
C- Risk management should not attend the workshop so that proper discussion can take place.
D- Compliance experts should not attend the workshop so that proper discussion can take place.

Answer:

B

Explanation:

Step 1: What Is a Risk Assessment Workshop?

A risk assessment workshop is a structured session where key stakeholders identify, evaluate, and prioritize risks.

Effective workshops require preparation, clear objectives, and structured discussions to ensure meaningful risk analysis.

Step 2: Why Option B is Correct

PRMIA and best practices recommend thorough preparation, including:

Setting objectives

Defining risk categories

Ensuring participation from risk, compliance, and business units

Providing risk assessment tools/templates

Step 3: Why the Other Options Are Incorrect

Option A ('Run spontaneously') Incorrect because lack of preparation leads to poor discussions and missed risks.

Option C ('Risk management should not attend') Incorrect because risk managers provide key expertise to guide discussions.

Option D ('Compliance experts should not attend') Incorrect because compliance provides regulatory insights essential to risk assessment.

PRMIA Risk Reference Used:

PRMIA Risk Assessment Framework -- Recommends structured, well-prepared workshops.

ISO 31000 Risk Management Standard -- Supports proactive workshop planning.

Final Conclusion:

Risk assessment workshops should be well-prepared to ensure meaningful discussions and effective risk identification, making Option B the correct answer.

Question 2

Question Type: MultipleChoice

Which of the follow does the risk function typically have responsibility for?

Options:

A- Documenting its activities, typically by operating and then recording the daily operation of controls.
B- Documenting its activities, typically by developing a Risk Management Manual and set of Risk Policies.
C- Putting in place the servers, firewalls and software to ensure cyber security.
D- Creating a trial balance, balance sheet statement and cash flow statement.

Answer:

B

Explanation:

Role of the Risk Function

The risk function is responsible for documenting, monitoring, and overseeing risk policies and frameworks.

It ensures the organization maintains structured risk governance, reporting, and compliance.

Key Responsibilities

Developing Risk Management Manuals to define risk appetite, risk frameworks, and risk governance structures.

Creating Risk Policies that align with regulatory standards and internal controls.

Why Answer B is Correct

The risk function primarily develops, implements, and maintains risk management frameworks, which include formal manuals and policies.

Why Other Answers Are Incorrect

Option

Explanation

A . Documenting its activities, typically by operating and then recording the daily operation of controls.

Incorrect -- The first line of defense (business units) handles daily operational controls, not the risk function.

C . Putting in place the servers, firewalls, and software to ensure cybersecurity.

Incorrect -- Cybersecurity is an IT responsibility, while the risk function oversees cyber risk frameworks.

D . Creating a trial balance, balance sheet statement, and cash flow statement.

Incorrect -- These are financial accounting responsibilities, not risk management duties.

PRMIA Reference for Verification

PRMIA Governance Framework for Risk Management

Basel Risk Management Principles

Question 3

Question Type: MultipleChoice

The The Task Force on Climate-related Financial Disclosures (TCFD) was founded by which body?

Options:

A- The World Bank (WB).

B- The United Nations (UN).
C- The Financial Stability Board (FSB).
D- The European Commission (EC).

Answer:

C

Explanation:

Step 1: What is the TCFD?

The Task Force on Climate-related Financial Disclosures (TCFD) was established to develop climate-related financial risk disclosure recommendations to help investors, lenders, and regulators make informed decisions.

Step 2: Who Founded the TCFD?

The Financial Stability Board (FSB), an international organization that monitors and makes recommendations about the global financial system, founded the TCFD in 2015.

The FSB recognized climate risk as a financial stability issue and launched the TCFD to standardize reporting.

Step 3: Why the Other Options Are Incorrect

Option A ('World Bank') Incorrect because the World Bank supports climate initiatives but did not create the TCFD.

Option B ('United Nations') Incorrect because the UN has climate programs like the UNFCCC, but not the TCFD.

Option D ('European Commission') Incorrect because the EC develops its own sustainability regulations (e.g., SFDR, CSRD), separate from the TCFD.

PRMIA Risk Reference Used:

PRMIA Climate Risk Guidelines -- Cites FSB's role in founding the TCFD.

FSB Official Reports (2015) -- Confirms that the FSB established the TCFD.

Final Conclusion:

The FSB founded the TCFD in 2015, making Option C the correct answer.

Question 4

Question Type: MultipleChoice

For the Northern Rock case study, what was the low-probability-high-impact event that was most responsible for the loss event?

Options:

A- The acquisition of Merrill Lynch by Bank of America.
B- The Bank of England's withdrawal of Deposit Protection.
C- Liquidity dried up in the inter-bank and commercial paper markets.
D- An exposure to real estate funds, heavily concentrated in Berlin.

Answer:

C

Explanation:

Step 1: Understanding the Northern Rock Case Study

Northern Rock was a UK bank that collapsed in 2007 due to its heavy reliance on short-term wholesale funding rather than customer deposits.

When the 2007 financial crisis hit, the inter-bank lending market and commercial paper market froze, cutting off Northern Rock's access to liquidity.

Step 2: Why Option C Is Correct

Northern Rock depended on short-term borrowing to fund long-term mortgage lending.

When the liquidity crisis hit, it couldn't refinance its debt, leading to a bank run and collapse.

The Bank of England had to intervene, and the UK government nationalized Northern Rock in 2008.

Step 3: Why the Other Options Are Incorrect

Option A ('Acquisition of Merrill Lynch') Incorrect because this happened in 2008, after Northern Rock's failure.

Option B ('Withdrawal of Deposit Protection') Incorrect because UK deposit protection remained in place.

Option D ('Real estate exposure in Berlin') Incorrect because Northern Rock's problem was funding liquidity, not real estate losses.

PRMIA Risk Reference Used:

PRMIA Liquidity Risk Management Framework -- Describes how liquidity shocks impact banks like Northern Rock.

Basel III Liquidity Coverage Ratio (LCR) Standards -- Created after Northern Rock to prevent similar liquidity crises.

Final Conclusion:

The collapse of the inter-bank and commercial paper markets was the key low-probability-high-impact event that led to Northern Rock's failure, making Option C the correct answer.

Question 5

Question Type: MultipleChoice

Ideally, Which option best should be completed as part of the risk assessments of service providers?

Options:

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.

Why Other Answers Are Incorrect

Option

Explanation

B . An assessment of a third party should not include its compliance and risk infrastructure, financials, business strategy, and operating history.

Incorrect -- Ignoring these critical factors increases the risk of working with an unreliable vendor.

C . Onsite visits are not advantageous for understanding the third party's risks and control environment.

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 the service.

Incorrect -- Employee salaries are not a primary risk 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.

Question 6

Question Type: MultipleChoice

How can a chief risk officer encourage the governing body and executive management team to create a stronger risk culture?

Options:

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 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.

Question 7

Question Type: MultipleChoice

Stafford Beers Viable System Model (VSM) has several implementation elements. Which of the following is not one of these?

Options:

A- Governance
B- Input
C- Process
D- Output

Answer:

B

Explanation:

Stafford Beer's Viable System Model (VSM)

VSM is a cybernetic model designed to analyze and improve organizational structures.

It consists of five core subsystems that define governance and operations.

Why Answer B is Correct

The VSM does not explicitly include ''Input'' as a key component.

The key elements of VSM include Governance, Process, and Output, but it does not define ''Input'' as a standalone concept.

Why Other Answers Are Incorrect

Option

Explanation

A . Governance

Correct -- Governance is part of VSM and deals with decision-making and oversight.

C . Process

Correct -- Process represents the operational functions within VSM.

D . Output

Correct -- Output refers to the results of the system's operations.

PRMIA Reference for Verification

PRMIA Governance and Cybernetic Systems Guidelines

Stafford Beer's Viable System Model Framework

Question 8

Question Type: MultipleChoice

Ideally, the facilitator of a risk assessment workshop should:

Options:

A- Guide the workshop toward a pre-determined conclusion, based upon known industry identified risks.
B- Remind the attendees that they can override the results of the workshop once the risks are tallied.
C- Remain objective and refrain from expressing his or her own opinions.
D- Attend via a video connection to allow proper distance.

Answer:

C

Explanation:

Step 1: Role of a Risk Assessment Facilitator

The facilitator's main role is to guide discussions without bias, ensuring objective risk identification.

PRMIA's Risk Governance Framework highlights neutral facilitation as key to effective risk workshops.

Step 2: Why Option C Is Correct

Objectivity ensures unbiased risk assessment.

Expressing personal opinions can influence risk ratings, leading to distorted outcomes.

Step 3: Why the Other Options Are Incorrect

Option A ('Guide the workshop toward a pre-determined conclusion')

Incorrect because risk workshops should discover risks, not confirm pre-set beliefs.

Option B ('Attendees can override results')

Incorrect as risk results should be evidence-based, not subject to override.

Option D ('Attend via video connection')

Incorrect as facilitators must engage actively, making remote facilitation less effective.

PRMIA Risk Reference Used:

PRMIA Risk Governance Framework -- Stresses objectivity in risk assessment facilitation.

PRMIA Risk Identification Best Practices -- Encourages unbiased workshops.

Final Conclusion:

Facilitators must remain neutral and objective, making Option C the correct answer.

Question 9

Question Type: MultipleChoice

Which of the follow is not included in PRMIA's 10 principles of good governance?

Options:

A- Risk appetite.
B- Holding the PRM Designation.
C- External validation.

D- Clear accountability.

Answer:

B

Explanation:

PRMIA's 10 Principles of Good Governance

PRMIA outlines 10 key principles that focus on risk governance, accountability, transparency, and risk management effectiveness.

These principles ensure strong risk governance structures for financial institutions.

Why Answer B is Correct

Holding the PRM Designation (Professional Risk Manager certification) is NOT a governance principle.

While PRMIA promotes risk education, governance principles focus on organizational risk structures, not individual certifications.

Why Other Answers Are Incorrect

Option

Explanation

A . Risk appetite.

Correct -- PRMIA governance principles include establishing a clear risk appetite.

C . External validation.

Correct -- External audits and validation improve governance and risk transparency.

D . Clear accountability.

Correct -- Governance principles emphasize clear accountability at all levels of management.

PRMIA Reference for Verification

PRMIA 10 Principles of Good Governance

Basel Corporate Governance Guidelines for Financial Institutions

Question 10

Question Type: MultipleChoice

For the Barings case study, what external event may have accelerated the discovery of the loss event?

Options:

A- The collapse of Lehman Brothers into bankruptcy in 2002.
B- The Singapore earthquake of January 17th 1995.
C- The collapse of Lehman Brothers into bankruptcy m 2008.
D- The Kobe earthquake of January 17th 1995.

Answer:

D

Explanation:

Background of the Barings Case Study

The Barings Bank collapse occurred due to unauthorized derivatives trading by Nick Leeson in Singapore.

Leeson concealed losses, and his trading positions became unmanageable.

How the Kobe Earthquake Affected Barings

On January 17, 1995, the Kobe earthquake caused extreme market volatility.

Leeson's unauthorized trades were highly exposed to the Nikkei 225 index, and the earthquake triggered heavy losses.

The event accelerated the exposure of Leeson's fraudulent activities, leading to Barings' collapse.

Why Answer D is Correct

The Kobe earthquake created market turmoil, forcing Barings to confront its financial position, ultimately revealing the hidden losses.

Why Other Answers Are Incorrect

Option

Explanation

A . The collapse of Lehman Brothers into bankruptcy in 2002.

Incorrect -- Lehman Brothers collapsed in 2008, not 2002.

B . The Singapore earthquake of January 17th, 1995.

Incorrect -- No significant earthquake occurred in Singapore on that date.

C . The collapse of Lehman Brothers into bankruptcy in 2008.

Incorrect -- Barings collapsed in 1995, not related to Lehman Brothers' 2008 failure.

PRMIA Reference for Verification

PRMIA Case Study on Barings Bank Collapse

Basel Committee Principles on Risk Oversight and Fraud Prevention

P2P exams

P2P exams

To Get Premium Files for 8020 Visit

https://www.p2pexams.com/products/8020

For More Free Questions Visit

https://www.p2pexams.com/prmia/pdf/8020

