201.Risk Management in Financial Institution (RMFI)

For AIBB

First Edition: September 2023
Second Edition: March 2024
Third Edition: June 2024
Fourth Edition: January 2025
Fifth Edition: June 2025
Sixth Edition: January 2026

Written By:

Mohammad Samir Uddin, CFA
CEO of a Reputed Asset Management Ltd
Former CEO of MBL Asset Management Ltd
Former Principal Officer of EXIM Bank Limited
CFA Chartered from CFA Institute, U.S.A.
BBA, MBA (Major in finance) From Dhaka University
Qualified in Banking Diploma and Diploma in Islami Banking
Course instructor: 10 Minute School of 96th BPE
Founder: MetaMentor Center,

Price: 350Tk.

For Order:
www.metamentorcenter.com
WhatsApp: 01310-474402

Metamentor Center
Unlock Your Potential Here.

Table of Content

Suggestion:

- ***Read 4 star and 5 star marked chapter if you have time shortage to read all chapter.***
- ***Must read short questions and difference from all chapter.***
- ***MetaMentor Center suggest to read whole note to find 100% common in exam. We cover everything in our note.***

Important	Details	Number of Question common in previous years
*****	Module-A: ***Introduction: Risk Management***	**23**
****	Module-B: ***Risk Identification and Assessment***	**19**
****	Module-C: ***Risk Management Responsibilities and Checklist***	**18**
**	Module-D: ***Operational risk Management***	**08**
**	Module-E: ***Steps of ERM Implementation***	**11**
*****	Module-F: ***Policy initiatives for development of risk management in FIs***	**30**
*****	Module-G: ***Implementation of Basel Capital Framework/Accord***	**37**
*****All short questions and difference from all chapter and end of note *****		

Syllabus

Module A: Introduction
Risk Management, Scope and concept of Risk Management and Enterprise Risk Management (ERM), Risk Culture, Risk Strategy, Risk Appetite and Tolerance, Risk Assessment and Treatment, Risk, Governance and Organization, Inherent Risk, Control, and Residual Risk.

Module B: Risk Identification and Assessment
Culture of Risk Identification, Process of Risk identification, Categorization of Risk, Financial Risks, Non-Financial Risks, Risk Assessment Techniques, Likelihood, Potential Impact, Selection of significant risks for the enterprise, Key Risk Indicators (KRI), Risk Register, Risk Rating.

Module C: Risk Management Responsibilities and Checklist
Elements of sound risk management system, Criteria for ensuring sound risk management. Role of Bank Supervisor and Regulator Board Oversight- Role of Board of Directors, Role of Board Risk Management Committee (BRMC). Senior Management Oversight- Role of Executive Risk Management Committee (ERMC) & its functions, Chief Risk Officer (CRO) - Appointment, Responsibilities & Functions, Risk Management Division (RMD) Roles & Functions. Role of other stakeholders for managing risks: Internal Stakeholders (like different risk committees, different units/cells), External Stakeholders (like regulatory authorities, statutory auditors, credit rating agencies, different development partners & lenders). Risk Management Checklist: Risk Architecture, Risk Strategy, Risk Protocol.

Module D: Operational risk Management
Operational Risk Management, its components & factors (People, Process, System etc.), Three (3) Lines of Defense (3LoDs), approach for managing operational risks, elements and parties of 3LoD, identification procedures, measurement, contingency planning etc.

Module E: Steps of ERM Implementation
Planning and Designing, Implementing and Benchmarking, Measuring and Monitoring, Learning and Reporting. Conducting stress testing - communicate its impact to Board & Senior management.

Module F: Policy initiatives for development of risk management in FIs
Core risk management initiated by Bangladesh Bank: Credit Risk Management (CRM), Asset-Liability Risk management (ALM), Foreign Exchange Risk Management (FX), Anti-Money Laundering Risk Management (AML), Internal Control & Compliance Risk Management (ICC), Information Communication & Technology Risk Management (ICT); Environmental & Social Risk Management (E&S risk Management).

Module G: Implementation of Basel Capital Framework/Accord
Basel Capital Framework issued by Bangladesh Bank: Components of capital (CET1, Tier 1, Tier 2), its importance for FIs, Limits-Maxima & Minima of capital ratios, Board and Senior Management oversight for managing sustainability of Capital, Capital Planning and dividend policy, relation between risk management and capital. Measurement of Risk Weighted Assets (RWA) under Pillar 1 for Credit risk, Market risk and Operational risk, Strategies for managing RWA of each segment. Measurement & Managing capital requirement for Pillar 2 – Supervisory Review Process, Preparation of ICAAP Documents for determination of capital requirement against different risks under Pillar 2. Pillar 3-Market Discipline: its importance for different stakeholders. Liquidity Ratios under Basel Capital Framework- Liquidity Coverage Ratio (LCR), Net Stable Funding Ratio (NSFR), Leverage Ratio-calculation procedures and importance for banks and NBFIs.

Module A:
Introduction: Risk Management

Q-01. What do you understand by risk? BPE-99th. BPE-5th.
Or, Explain the 'Risk' considering the activities of a financial institution. BPE-98th.
Risk refers to the possibility of uncertain outcomes or negative events that could impact the success or stability of a bank or financial institution. It involves the potential for financial losses, reputation damage, or operational disruptions. For example, a bank may face the risk of default on loans if borrowers fail to repay their debts. This could result in financial losses for the bank and affect its ability to meet its obligations. Managing risk involves implementing strategies and safeguards to mitigate potential negative impacts and protect the institution's assets and reputation.

Q-02. What is the relationship between risk and returns? BPE-97th.
Risk and return are closely related in finance. Generally, higher-risk investments offer the potential for higher returns, while lower-risk investments typically yield lower returns. This relationship is based on the principle that investors need to be compensated for taking on additional risk. For example, a government bond, considered low risk, usually offers a modest return. In contrast, stocks, that are riskier due to market volatility and uncertainty, often provide the chance for higher returns. Investors balance these elements to align with their risk tolerance and investment goals. In summary, the risk-return tradeoff is a fundamental concept, where higher risk is associated with the potential for higher rewards, and vice versa.

Q-03. What do you understand by risk management? BPE-97th. BPE-99th.
Risk management involves identifying, assessing, and prioritizing risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events. It's a strategy to manage uncertainty in investment decisions, ensuring potential threats are understood and mitigated while opportunities are maximized. This process is crucial in business and investing, as it helps organizations and investors avoid or reduce losses. Effective risk management strategies include diversification, hedging, insurance, and setting aside emergency funds. By systematically managing risks, individuals and organizations can protect their assets, ensure stability, and achieve their objectives more reliably. It's about making informed decisions to navigate uncertainties in any endeavor.

Q-04. Briefly describe the risks involved in banking book, trading book and off-balance sheet exposure.
Or, Business Line from Risk Management Perspective.
In a bank, different types of activities carry different risks:

1. **Banking Book:** This is where the bank keeps track of long-term stuff like loans and mortgages. The main risk here is credit risk—people not paying back their loans. Interest rate changes can also be a risk, affecting how much the bank earns from these loans.
2. **Trading Book:** This is the bank's short-term financial activities, like buying and selling stocks or bonds. Market risk is the big concern here. If market prices move the wrong way, the bank could lose money quickly.
3. **Off-Balance Sheet Exposure:** These are deals the bank makes that don't show up on the main financial statements, like guarantees or derivatives. Risks here are often hidden and can include both credit risk and market risk. Plus, these are hard to keep track of, so there's a risk of surprise losses.
4. Each area needs careful management to keep the bank stable and profitable.

Understanding and managing these risks are essential for banks to ensure financial stability and resilience.

Q-05. What kind of change do you think is required in the current risk management system in your organization? BPE-96th.

For the banking industry in Bangladesh to enhance its risk management system, several changes are crucial:

1. **Technology Upgrade**: Implementing advanced technology for real-time risk monitoring and analytics can significantly improve risk detection and management capabilities.
2. **Regulatory Compliance**: Strengthening compliance with international banking standards (like Basel III) to ensure robust capital adequacy, stress testing, and liquidity management.
3. **Risk Culture**: Cultivating a strong risk culture across all levels of the organization, where risk awareness and management are integral to daily operations.
4. **Training and Development**: Investing in regular training programs to equip staff with the latest risk management techniques and practices.
5. **Integrated Risk Management**: Adopting a holistic approach to risk management that encompasses credit, market, operational, and other risks in a unified framework.
6. **Cybersecurity Measures**: Enhancing cybersecurity protocols to protect against increasing digital threats and ensuring data integrity and security.
7. These changes can help mitigate risks more effectively, ensuring the banking sector's stability and growth.

Q-06. Discuss your role in risk management considering the risks of your bank. BPE-98th.

In the role of an official in the credit department, managing risks effectively involves:

1. **Credit Risk Management**: Assessing borrowers' creditworthiness, ensuring compliance with lending policies, and maintaining portfolio quality to minimize defaults.
2. **Monitoring and Reporting**: Regularly reviewing loan performance and promptly reporting potential risks to senior management.
3. **Risk Mitigation Strategies**: Applying safeguards such as collateralization, guarantees, or credit derivatives to reduce exposure to credit risks.
4. **Policy Adherence**: Implementing the bank's risk management framework and adhering to regulatory guidelines to align with risk appetite.
5. **Proactive Assessment**: Identifying emerging risks and adapting strategies to mitigate potential impacts.

Q-07. Do you think that supervisors and regulators proper initiatives are the only way to ensure sound risk management systems in an organization? BPE-96th.

While supervisors and regulators play a crucial role in establishing guidelines and standards for risk management, they are not the sole factor ensuring sound risk management systems in an organization. Effective risk management also depends on:

1. **Regulatory Role:** Supervisors and regulators establish guidelines and compliance standards for risk management.
2. **Not the Sole Solution:** Effective risk management requires more than just regulatory compliance.
3. **Organizational Culture:** A risk-aware culture encourages all employees to participate in identifying and mitigating risks.
4. **Leadership Commitment:** Leadership must prioritize risk management and allocate resources appropriately.
5. **Employee Training:** Ongoing training ensures employees understand risk management practices and their roles.
6. **Internal Controls:** Strong internal controls are essential for monitoring and managing risks effectively.
7. **Continuous Monitoring:** Regular assessments help in adapting to new risks and improving risk management strategies.
8. **Proactive Measures:** Organizations should take proactive steps beyond regulatory requirements to manage risks.

Effective risk management combines regulatory guidance with an organization's internal efforts to create a comprehensive approach.

Q-08. How does the active participation of the board of directors and senior management contribute effectively to the sound risk management of a financial institution? Explain. BPE-97th.

The active participation of the board of directors and senior management is paramount in fostering effective risk management within a financial institution.

1. **Strategic Alignment**: Board and senior management involvement ensures that risk management strategies align with the institution's overall objectives, preventing conflicts between risk-taking and organizational goals.
2. **Risk Culture**: Leadership sets the tone for a risk-aware culture. Their commitment to ethical practices and risk consciousness permeates throughout the organization, promoting a robust risk management environment.
3. **Decision-Making Oversight**: Boards and senior management provide oversight on major decisions, ensuring that risks are adequately considered and that risk-taking activities are within acceptable limits.
4. **Resource Allocation**: Effective risk management requires resource allocation. Board and senior management involvement ensures the allocation of adequate resources for risk identification, assessment, and mitigation.
5. **Compliance and Governance**: Leadership's active role ensures compliance with regulations and governance standards, mitigating legal and regulatory risks.

In summary, the engagement of the board and senior management establishes a risk-aware culture, aligns strategies with objectives, and provides the necessary oversight and resources for sound risk management in financial institutions.

Q-09. Discuss the scope of Risk Management.

The scope of risk management is about what areas you're going to focus on to keep things running smoothly. For a bank, this can include:

1. **Credit Risk:** Making sure people who borrow money can pay it back.
2. **Market Risk:** Watching how changes in interest rates or stock prices could affect the bank.
3. **Operational Risk:** Making sure the bank's systems, like computers and customer service, work well.
4. **Compliance Risk:** Following all the laws and rules that banks have to obey.
5. **Strategic Risk:** Planning for the long-term, like what services to offer or markets to enter.
6. **Reputation Risk:** Managing how people see the bank, so customers keep trusting it.

So, the scope covers everything from daily operations to long-term planning, making sure the bank stays healthy, compliant, and trusted.

Q-10. Briefly discuss the Enterprise Risk Management (ERM). BPE-6th.

Enterprise Risk Management (ERM) is a strategic framework that allows organizations to identify, assess, and prepare for potential risks affecting operations and objectives. Unlike traditional siloed approaches, ERM takes a holistic view, integrating risk management across all departments and business units.

Key aspects of ERM include:

1. **Holistic Approach**: Risks are evaluated collectively to ensure alignment with organizational goals.
2. **Integration**: Incorporates credit, market, operational, and liquidity risks under a single framework.
3. **Proactive Planning**: Identifies and mitigates risks before they materialize.
4. **Strategic Decision-Making**: Helps in balancing risk appetite with business opportunities.

For example, a bank using ERM might assess credit risks across branches and consolidate insights to manage its risk exposure more effectively, ensuring compliance with regulatory frameworks like Basel norms.

Q-11. Describe the benefits of maintaining effective Enterprise Risk Management (ERM)?

1. Maintaining effective Enterprise Risk Management (ERM) provides several benefits:
2. **Proactive Protection:** Identifying and mitigating risks in advance, protecting the organization from potential threats.
3. **Informed Decision-Making:** Providing data-driven insights to make well-informed and strategic decisions.
4. **Resilience:** Strengthening the organization's ability to adapt and recover from unexpected events and uncertainties.
5. **Resource Optimization:** Efficiently allocating resources to manage risks, maximizing effectiveness and cost-saving.
6. **Stakeholder Confidence:** Building trust and confidence among stakeholders by demonstrating responsible risk management practices.
7. **Sustainable Growth:** Supporting long-term success and sustainability by considering risks in strategic planning.
8. **Compliance:** Ensuring adherence to laws, regulations, and industry standards, reducing legal and reputational risks.
9. Effective ERM enhances organizational stability, performance, and the ability to capitalize on opportunities while minimizing potential negative impacts.

Q-12. Define risk culture? Why should risk culture be given due importance? BPE-99th.

Or, Discuss how important the risk culture is for effective bank management. BPE-97th.

Risk culture refers to the values, attitudes, and behaviors within an organization regarding risk awareness and management. It reflects how employees perceive and respond to risks, impacting their decisions and actions.

Importance: Risk culture should be given due importance because it directly influences an organization's ability to identify and handle risks effectively. A positive risk culture promotes transparency, open communication, and accountability, encouraging employees to be proactive in reporting and addressing risks. When risk culture is prioritized, it fosters a risk-aware environment, enabling better decision-making, early risk detection, and the ability to adapt to uncertainties. By nurturing a strong risk culture, organizations can minimize potential negative impacts, enhance resilience, and achieve sustainable success in an ever-changing business landscape.

Q-13. Discuss the Process for Managing Risk Culture.

To manage risk culture effectively, organizations should follow a structured process that includes:

1. **Define/Steer Target Risk Culture**:
   a. Establish a clear view of the desired risk culture.
   b. Identify the specific attitudes and behaviors necessary to align with organizational goals.
2. **Measure Current State**:
   a. Assess the existing risk culture using surveys, audits, and employee feedback to determine strengths and weaknesses.
3. **Gap Analysis**:
   a. Compare the current state with the desired culture to identify gaps and areas for improvement.
4. **Design Corrective Actions**:
   a. Develop and implement targeted measures, such as training programs, communication plans, and revised policies, to bridge the identified gaps.

Example: A bank may measure its employees' understanding of risk policies and identify a gap in awareness. Corrective action might include specialized training sessions to improve compliance and risk awareness.

Q-14. Mention some areas where bank should have their own risk strategy.

1. **Credit Risk:** Managing the risk of borrowers defaulting on loans or credit products.
2. **Market Risk:** Addressing potential losses due to fluctuations in interest rates, foreign exchange rates, or market prices.
3. **Operational Risk:** Mitigating risks arising from internal processes, systems, or human error.
4. **Liquidity Risk:** Ensuring sufficient funds to meet financial obligations and handle unforeseen events.
5. **Compliance Risk:** Adhering to regulatory requirements and avoiding penalties.
6. **Reputational Risk:** Safeguarding the bank's image and brand reputation.
7. **Cybersecurity Risk:** Protecting against cyber threats and data breaches.
8. **Strategic Risk:** Evaluating potential risks associated with business strategies and decisions.

Q-15. What is risk appetite? Why is developing risk appetite statement help in mitigating the risk? BPE-96th. BPE-98th. BPE-99th.

Risk appetite is like how much spicy food you're willing to eat; it's the amount of risk a company is comfortable taking on to achieve its goals. In a business context, a Risk Appetite Statement is like saying, "We're okay with a little spice, but not too much."

Why is it helpful?

1. **Clear Limits:** The statement sets clear boundaries on what kinds of risks are okay and how much risk are too much.
2. **Informed Decisions:** Knowing the risk appetite helps managers make better choices that align with the company's comfort level for risk.
3. **Team Alignment:** Everyone in the company understands what the acceptable level of risk is, making it easier to work together.
4. **Risk Control:** By knowing your limits, you can avoid taking on too much risk that could harm the company.
5. **Trust:** Shareholders and customers feel more confident if they know the company has a well-defined approach to managing risks.

So, having a Risk Appetite Statement helps the company manage risks more effectively and keeps everyone on the same page.

Q-16. Discuss the relationship between risk appetite and risk response strategy of a bank. BPE-98th.

Think of risk appetite as a bank's hunger for risk and risk response strategy as its plan for dealing with that hunger. Here's how they're related:

1. **Understanding Hunger**: Risk appetite helps a bank figure out how much risk it's willing to take to meet its goals. It's like deciding how spicy you want your food – some banks like it mild, while others prefer it hot.
2. **Choosing the Menu**: Once the bank knows its appetite, it picks a risk response strategy. This is like choosing what dishes to order based on how much spice you can handle. If the bank has a low risk appetite, it might go for safer options, while a high-risk appetite might lead to more adventurous choices.
3. **Balancing Flavors**: The risk response strategy should match the bank's risk appetite. It's like making sure the food matches your taste buds – too much spice can be uncomfortable, just like too much risk can be dangerous.

By aligning risk appetite with the risk response strategy, banks can ensure they're taking the right amount of risk to achieve their goals without getting burned.

Q-17. What the objectives of risk appetite? BPE-98th.

1. The objectives of risk appetite are to:
2. **Set Boundaries:** Clearly define the level of risk the organization is willing to accept to achieve its objectives.
3. **Guide Decision-Making:** Provide a framework for making informed decisions about risk-taking and risk management.
4. **Enhance Resilience:** Ensure the organization's ability to withstand adverse events within acceptable risk parameters.
5. **Align with Strategy:** Ensure that risk-taking aligns with the organization's overall strategic goals and objectives.
6. **Prioritize Risks:** Assist in prioritizing risks based on their significance and potential impact on the organization.
7. **Optimize Risk Management:** Facilitate the allocation of resources to effectively manage and mitigate risks.

Overall, risk appetite ensures a balanced approach to risk-taking, promoting stability, and supporting the organization's long-term success.

Q-18. Discuss the elements/components of the risk appetite framework.

A bank's Risk Appetite Framework (RAF) should encompass several essential components:

1. **Board Approval**: Reviewed and approved by the board of directors at least annually.
2. **Alignment with Strategy**: Align with the organization’s strategy, objectives, and stakeholders’ demands.
3. **Comprehensive Coverage**: Cover all key risks, including preferences for both desired and minimized risks.
4. **Risk Documentation**: Clearly document risks in a risk register, including definitions, risk owners,

measurement frequency, assumptions, severity, likelihood, and manifestation speed.

5. **Loss Tolerances**: Recognize that losses are part of business and include tolerances reflecting overall
   business objectives.
6. **Resource Allocation**: Reflect the human and technological resources needed to measure and manage risks
   timely.

Q-19. Discuss how to develop and adopt a risk appetite framework (RAF) in a bank.

To develop and adopt a Risk Appetite Framework (RAF) in a bank:

1. **Assess Current Risk Profile:** Evaluate existing risks, risk management practices, and risk tolerance levels.
2. **Define Risk Tolerance:** Establish clear risk tolerance thresholds for different risk categories.
3. **Involve Stakeholders:** Engage key stakeholders, including senior management and board members, to gain buy-in and input.
4. **Establish Risk Limits:** Set specific risk limits and key risk indicators to monitor risk exposures.
5. **Communication:** Effectively communicate the RAF throughout the organization to ensure understanding and alignment.
6. **Implement and Monitor:** Integrate the RAF into decision-making processes and regularly review its effectiveness.
7. **Continuous Improvement:** Adapt the RAF as the bank's risk profile and strategic objectives evolve.

Adopting an effective RAF empowers the bank to make informed decisions, enhance resilience, and achieve its business objectives while managing risks prudently.

Q-20. What do you mean by risk assessment? What are the most common risk assessment techniques used by banks? BPE-5th.

Risk assessment is the process of identifying, analyzing, and evaluating potential risks that could affect an individual, organization, or project. It involves understanding the likelihood of a risk occurring and the potential impact it may have. The goal of risk assessment is to assess the significance of risks to prioritize and plan appropriate risk management strategies. By conducting risk assessments, individuals and organizations can make informed decisions to mitigate, avoid, or prepare for potential negative consequences, enhancing their ability to navigate uncertainties and achieve their goals more effectively.

For instance, before opening a new restaurant, a risk assessment would involve identifying possible risks like food safety, customer satisfaction, and competition. The assessment would analyze the likelihood of these risks occurring and their potential consequences.

Based on this information, the restaurant owner can develop strategies to address each risk, such as implementing rigorous food safety protocols, conducting customer surveys, and offering unique menu items to stand out from competitors. Risk assessment helps businesses anticipate challenges and plan for success while minimizing potential negative outcomes.

Banks use different techniques to find, measure, and understand risks in their operations. Common techniques are:

1. **Risk Control Self-Assessment (RCSA)** – Staff assess risks and controls within their own departments.
2. **Scorecards** – These rate risks using weighted scores to compare risk levels across departments.
3. **Quantitative Analysis** – Uses numbers, data, and models (like Monte Carlo simulation) to measure risk.
4. **Qualitative Analysis** – Relies on expert judgment and experience when data is not available.
5. **Risk Likelihood and Impact Matrix** – Shows how likely a risk is and how much damage it can cause.
6. **Key Risk Indicators (KRIs)** – Early warning signals that show rising or potential risks.

Q-21. What do you mean by risk treatment? Discuss different risk treatment options/strategies. BPE-98th.

Or, Explain the risk treatment strategies typically adopted by banks.BPE-6th.

Risk treatment refers to the process of selecting and implementing measures to manage or mitigate identified risks effectively. It aims to reduce the likelihood or impact of risks to an acceptable level. Different risk treatment options include:

1. **Avoidance:** Eliminating activities or exposures that pose high risks to prevent their occurrence.
2. **Reduction:** Implementing controls and preventive measures to minimize the likelihood or impact of risks.
3. **Transfer:** Shifting the responsibility for risk to another party, such as insurance or outsourcing.
4. **Acceptance:** Acknowledging and consciously deciding to bear the risk, often applicable to lower-level risks.
5. **Diversification:** Spreading investments or exposures across various areas to reduce concentrated risks.
6. **Contingency Planning:** Developing response plans to handle and recover from unexpected events.

Q-22. Considering the severity and probability of occurrence, how risk should be treated?

Considering the severity and probability of occurrence, risks should be treated in a way that aligns with the organization's risk appetite. Different risk treatment options based on risk severity and probability include:

1. **High Severity, High Probability:** Risks with severe consequences and high likelihood should be treated with priority. Measures like avoidance, reduction, or transfer may be appropriate.
2. **High Severity, Low Probability:** Risks with severe impacts but low chances of occurring may benefit from contingency planning or acceptance.
3. **Low Severity, High Probability:** Risks with minor consequences but high likelihood can be managed through reduction or acceptance.
4. **Low Severity, Low Probability:** Risks with minor impact and low chances of occurring may be accepted without additional treatment.

By tailoring risk treatment based on severity and probability, organizations can allocate resources efficiently, focusing efforts on managing significant risks while accepting lower-level risks that are manageable without excessive measures. This approach optimizes risk management efforts and supports the organization's overall objectives.

Q-23. Discuss the three lines of defense model in risk management.

The three lines of defense model in risk management is a framework that helps organizations effectively manage risks.

First Line of Defense: This involves the front-line operational staff responsible for daily activities. They identify and manage risks within their areas, ensuring proper controls and compliance.

Second Line of Defense: This comprises risk management, compliance, and internal control functions. They oversee and support the first line, ensuring risk frameworks are in place, and policies are followed.

Third Line of Defense: The internal audit function operates independently from the first and second lines. They assess risk management effectiveness and verify if controls are working as intended. This model ensures a clear division of responsibilities and provides checks and balances to manage risks efficiently. It strengthens risk management practices, promotes accountability, and enhances the organization's overall risk management capabilities.

Q-24. What is a risk governance framework?

A risk governance framework outlines the structure and processes for managing risks within an organization. It defines the roles, responsibilities, and communication channels for effective risk management. Key roles and functions in a risk governance framework include:

1. **Board of Directors:** Setting risk appetite, overseeing risk management, and ensuring alignment with strategic goals.
2. **Risk Committee:** Assisting the board in risk oversight and providing expertise in risk assessment and mitigation.
3. **Chief Risk Officer (CRO):** Leading the risk management function and coordinating risk-related activities.
4. **Risk Owners:** Identifying and managing risks within their respective areas of responsibility.
5. **Risk Management Function:** Developing risk policies, methodologies, and frameworks, and supporting risk analysis and treatment.

Q-25. How can effective corporate governance help to mitigate risk in a bank? BPE-98th.

Effective corporate governance is like having good captains on a ship, guiding it safely through rough waters. Here's how it helps banks manage risks:

1. **Clear Direction**: Good governance sets out rules and guidelines for how the bank should operate, including managing risks.
2. **Accountability**: It ensures that everyone in the bank, from top executives to employees, is responsible for their actions. This encourages careful decision-making and reduces the chances of risky behavior.
3. **Transparency**: Banks with strong governance practices are open and honest about their operations and risks. This helps investors, regulators, and customers trust the bank more.
4. **Risk Oversight**: Good governance involves regular monitoring and assessment of risks by the board of directors. They can identify potential problems early and take action to prevent them from getting worse.

Overall, effective corporate governance creates a culture of responsibility and transparency, making banks more resilient to risks.

Q-26. Discuss how to implement the three lines of defense model of a bank appropriately.

To implement the three lines of defense model in a bank effectively:

1. **Clearly Define Roles:** Define the responsibilities of each line of defense, ensuring a clear division of tasks.
2. **Establish Communication:** Promote open communication and collaboration between the three lines, fostering a culture of risk awareness.
3. **Provide Training:** Offer training and support to employees in each line to enhance their understanding of risk management.
4. **Develop Risk Framework:** Create a comprehensive risk framework with policies, procedures, and risk assessment methodologies.

5. **Monitor and Review:** Regularly assess the effectiveness of the model, identifying areas for improvement and adjusting as needed.
6. **Engage Leadership:** Gain support from senior management to endorse and champion the three lines of defense model.
7. **Internal Audit Independence:** Ensure the internal audit function remains independent to provide unbiased evaluations.

By following these steps, the bank can successfully implement the three lines of defense model, strengthening risk management practices and promoting a resilient and compliant organization.

Q-27. What is the benefits bank three-line defense model?
Or, Discuss the importance of 'Three Lines of Defense (3LoD)' in operational risk management. BPE-98th.

1. The three lines of defense model offers several benefits to banks:
2. **Enhanced Risk Management:** Clearly defining roles and responsibilities ensures risks are identified, managed, and monitored effectively.
3. **Improved Governance:** The model promotes accountability and transparency, enhancing corporate governance practices.
4. **Strong Compliance:** It helps banks adhere to regulatory requirements and industry standards, reducing compliance-related risks.
5. **Efficient Operations:** By having specialized teams, it ensures focus on their core functions, leading to efficient operations.
6. **Effective Internal Controls:** The model provides independent validation of controls, ensuring they work as intended.
7. **Stakeholder Confidence:** The model builds trust among stakeholders, demonstrating robust risk management practices.
8. **Early Risk Detection:** It allows for early identification of emerging risks, enabling timely risk mitigation.

The three lines of defense model ultimately supports the bank's stability, resilience, and ability to navigate challenges in an ever-changing financial landscape.

Q-28. What do you mean by Inherent Risk?
Or, Write Short note on: Inherent risk. BPE-5th.

Inherent Risk refers to the level of risk that exists naturally in a situation or activity before any measures are taken to mitigate it. It is the potential impact of an event multiplied by its likelihood of occurring.

For example:

1. **Cybersecurity Risk**: If an organization conducts online transactions without firewalls or antivirus software, the inherent risk of a cyberattack is extremely high.
2. **Employee Risk**: More employees can mean higher chances of errors or fraud. Without checks like vetting or monitoring, this risk remains high.

3. **Vendor Risk**: Allowing vendors access to sensitive systems can introduce risks. Without controls like vendor management, the institution faces significant inherent risk.

Inherent risk assessment helps organizations prioritize risks and plan safeguards effectively

Q-29. What do you mean by Risk control?

Risk control refers to the measures and actions taken to minimize, mitigate, or manage risks effectively within an organization. It involves implementing policies, procedures, and tools to prevent potential losses or reduce their impact. For example, a bank may use firewalls and encryption software to safeguard its digital systems from cyberattacks. Similarly, ensuring proper segregation of duties in financial transactions helps prevent fraud. Regular monitoring and assessment of controls ensure they remain effective and relevant, adapting to new risks as they arise. Risk control is critical for maintaining operational efficiency, protecting assets, and achieving organizational goals.

Imagine a bank's credit department is assessing loans. To control the risk of default, the bank implements a policy that requires checking the borrower's credit history and financial stability before approving a loan. This control helps minimize the likelihood of lending to individuals who may not repay, thereby protecting the bank's assets.

Q-30. What do you mean by Residual risk?

Residual risk refers to the level of risk that remains after applying controls or mitigation strategies. It acknowledges that no control is entirely effective in eliminating risk. Residual risk can result from factors like partial control effectiveness, unforeseen events, or the nature of the risk itself.

The corrected formula based on your attached file is:

Residual Risk = Inherent Risk × Control Effectiveness

Where:

- **Inherent Risk** is the level of risk before any controls are applied.
- **Control Effectiveness** represents how well the controls reduce the risk.

Example: If the **Inherent Risk** is 100 and the **Control Effectiveness** is 0.8 (80%), the **Residual Risk** would be:

Residual Risk = 100 × 0.8 = 80

This highlights the importance of monitoring and managing the risk that remains even after applying controls.

Q-31. Outline effective strategies that a financial institution can implement to reinforce and enhance its risk culture. BPE-99th.

Effective strategies for financial institutions to reinforce and enhance risk culture include:

1. **Define Target Risk Culture**: Establish a clear understanding of the desired risk culture aligning with organizational objectives.
2. **Measure Current Culture**: Assess and identify gaps between the current and target risk culture.

3. **Design Corrective Actions**: Develop actionable strategies to bridge the identified gaps.
4. **Promote Open Communication**: Foster an environment where employees feel confident to report risks without fear.
5. **Integrate Risk into Decision-Making**: Embed risk awareness in everyday operations and strategic planning.
6. **Provide Training**: Educate employees about their roles and responsibilities in risk management.
7. **Align Incentives with Objectives**: Ensure rewards and penalties reflect adherence to risk management principles.

Example: A bank introduces a whistleblower policy encouraging staff to report unethical practices, enhancing accountability and trust

Q-32. Discuss the role of Internal Audit Department in risk management. BPE-97th.

The role of the Internal Audit Department in risk management includes:

- **Policy Compliance**: Ensures adherence to board-approved policies and procedures.
- **Control Assessment**: Evaluates the effectiveness of internal control and governance systems.
- **Risk Monitoring**: Tests and monitors risk measures for alignment with organizational goals.
- **Risk-Based Audits**: Conducts audits focusing on critical risk areas.
- **Regulatory Compliance**: Checks compliance with internal policies and external regulations.
- **Communication Enhancement**: Acts as a bridge between the board and management for risk-related issues.
- **Recommendations**: Provides actionable insights to improve risk management systems.

These functions enhance the organization's ability to identify, assess, and mitigate risks effectively.

Q-33. A sound risk management policy will not work if the bank management does not recognize the policy in their day to day activities— please write your opinion on this statement. BPE-5th.

1. This statement is true. A bank may have a strong risk management policy, but it will fail if the management
   does not apply it daily.
2. A written risk policy is useless if not applied in day-to-day operations.
3. Bank management must **actively follow** and enforce the policy in all activities.
4. **Senior management and staff** should use the policy during lending, investing, and internal processes.

5. Without daily use, **risks remain unchecked**, which may lead to financial loss or non-compliance.
6. A **risk-aware culture** must be built through regular training and communication.
7. **Monitoring, reporting, and accountability** should be maintained to ensure proper policy use.
8. Board oversight and proper **governance structure** are key to linking policy with practice.

Case Study

Case–1 (Risk Appetite, Risk Culture, and ERM Governance)

Case Scenario:

UGC Bank PLC has grown rapidly in the last 2 years by expanding SME lending and launching new digital products. However, the bank has not updated its Risk Appetite Statement, and business units are approving new loans based mainly on growth targets. The Risk Management Division (RMD) reports that early warning signals are increasing, such as rising overdue loans in SME, frequent policy exceptions, and customer complaints about aggressive recovery practices. The Board Risk Management Committee (BRMC) meets irregularly and receives only descriptive reports without Key Risk Indicators (KRIs). The bank's culture encourages "business growth first," and staff rarely report issues due to fear of negative performance ratings. Recently, Bangladesh Bank asked the bank to explain how its risk appetite and risk strategy align with its business expansion plan.

Required:

Q-01. Identify the key risk management problems in this bank considering risk culture, risk strategy, and risk appetite.

Q-02. Classify the major risks into financial and non-financial risks and explain why they are significant.

Q-03. Propose KRIs and a risk register structure that would help management monitor these risks.

Q-04. Recommend short-term corrective actions and long-term ERM reforms, including the roles of Board, BRMC, ERMC, CRO, and RMD.

Answer:

Q-01. Key risk management problems related to risk culture, risk strategy, and risk appetite

UGC Bank PLC is facing several risk management problems

- The bank has expanded SME lending and digital products **without updating the Risk Appetite Statement**, so the acceptable level of risk is not clearly defined.
- The **risk culture is weak** because employees give priority to business growth instead of risk control.
- The **risk strategy is not aligned with the business strategy**, as loan approvals are mainly based on growth targets rather than proper risk assessment.

- The **Board Risk Management Committee (BRMC)** meets irregularly and does not perform effective risk oversight.
- The bank does not use **Key Risk Indicators (KRIs)**, which limits early detection and monitoring of emerging risks.

Q-02. Classification of major risks into financial and non-financial risks

Financial Risks:

- **Credit Risk:** Rising overdue SME loans show increased risk of default, which can reduce profitability and capital.
- **Liquidity Risk**: Aggressive lending growth without proper control can put pressure on cash flow.

Non-Financial Risks:

- **Operational Risk:** Frequent policy exceptions and weak internal controls increase the chance of process failures.
- **Reputation Risk:** Customer complaints about aggressive recovery practices damage public trust.
- **Compliance Risk:** Misalignment with Bangladesh Bank guidelines may lead to regulatory penalties.

These risks are significant because they can affect the bank's stability, regulatory standing, and long-term sustainability.

Q-03. Proposed KRIs and risk register structure

Proposed Key Risk Indicators (KRIs):

- Percentage of overdue SME loans
- Number of policy exceptions approved
- Volume of customer complaints
- Frequency of recovery-related disputes
- Growth rate of loans versus approved risk appetite limits

Risk Register Structure:

- Risk category (credit, operational, compliance, reputation)
- Risk description
- Risk owner (business unit or RMD)
- Likelihood and impact level
- Existing controls
- KRIs and thresholds
- Mitigation actions and review date

This structure helps management monitor risks in a systematic and timely manner.

Q-04. Short-term corrective actions and long-term ERM reforms

Short-term actions:

1. Update the Risk Appetite Statement immediately.

2. Introduce KRIs and submit them regularly to BRMC.
3. Strengthen SME credit review and early warning systems.
4. Encourage staff to report issues without fear of punishment.

Long-term ERM reforms:

1. **Board:** Approve risk appetite, oversee ERM, and ensure alignment with strategy.
2. **BRMC:** Hold regular meetings and review risk dashboards with KRIs.
3. **ERMC:** Coordinate enterprise-wide risk identification and mitigation.
4. **CRO:** Lead risk governance, ensure independence of RMD, and report directly to the Board.
5. **RMD:** Monitor risks, maintain risk register, and support business units with risk analysis.

Case –2: (Operational Risk, Three Lines of Defense, and Internal Control)

Case Scenario:

MZX Bank PLC recently faced repeated operational incidents in several branches. These include wrong posting of transactions, delayed reconciliation of suspense accounts, frequent system downtime, and a case of internal fraud involving fake account opening and unauthorized fund transfers. Internal audit reports repeatedly pointed out poor segregation of duties, weak maker-checker controls, and lack of monitoring of privileged system access. However, branch management treated these findings as "routine issues" and did not implement corrective actions. The Compliance and Internal Control unit issued warnings, but follow-up was weak. Bangladesh Bank's inspection team noted that the bank's three lines of defense are not functioning properly and requested an action plan to strengthen operational risk management and internal controls.

Required:

Q-01. Identify the operational risk factors under people, process, system, and external events in this case.

Q-02. Explain how weaknesses in the three lines of defense contributed to repeated incidents.

Q-03. Recommend immediate corrective controls to reduce inherent risk and residual risk in branches.

Q-04. Propose a sustainable operational risk management framework, including incident reporting, RCSA, KRIs, contingency planning, and internal audit follow-up.

Answer:

Q-01. Operational risk factors under people, process, system, and external events

People risk:

- Employees were involved in fake account opening and unauthorized fund transfers.
- Staff lacked adequate training and awareness about internal control and compliance.
- Negligence by branch management in taking audit observations seriously increased risk.

Process risk:

- Poor segregation of duties between maker and checker functions.
- Delayed reconciliation of suspense accounts.
- Weak follow-up on internal audit and compliance findings.

System risk:

- Frequent system downtime disrupted normal banking operations.
- Weak control over privileged system access increased the chance of misuse.

External event risk:

- Regulatory risk increased due to Bangladesh Bank inspection findings.
- Reputational risk arose from fraud and service disruption affecting customer trust.

Q-02. Role of weaknesses in the Three Lines of Defense

- **First Line of Defense (Business Units):** Branches failed to maintain proper controls and treated control weaknesses as routine issues.
- **Second Line of Defense (Compliance and Internal Control):** Although warnings were issued, monitoring and follow-up were weak and ineffective.
- **Third Line of Defense (Internal Audit):** Repeated audit findings were not resolved, showing weak enforcement and escalation.

As a result, control failures continued and operational incidents repeated.

Q-03. Immediate corrective controls to reduce inherent and residual risk

- Enforce strict maker-checker and segregation of duties in all branches.
- Ensure daily reconciliation of suspense and transit accounts.
- Restrict and monitor privileged system access regularly.
- Take disciplinary action against employees involved in fraud.
- Conduct urgent staff training on operational risk and internal control.
- Ensure prompt implementation of audit and compliance observations.

Q-04. Sustainable operational risk management framework

1. **Incident Reporting:** Establish a formal system to record, report, and analyze operational loss events.
2. **Risk and Control Self-Assessment (RCSA):** Branches should regularly identify operational risks and
   assess control effectiveness.
3. **Key Risk Indicators (KRIs):** Use indicators such as number of posting errors, system downtime, and overdue reconciliations.
4. **Contingency Planning:** Prepare and test business continuity and disaster recovery plans.
5. **Internal Audit Follow-up:** Ensure strict tracking and closure of audit findings with management accountability.

This framework will help MZX Bank PLC strengthen operational risk management and meet Bangladesh Bank regulatory expectations.

Compare And Contrast

Q-01. What is the difference between risk management and risk assessment?

Criteria	Risk Management	Risk Assessment
1.Definition	Risk Management is the systematic process of identifying, analyzing, and mitigating risks to achieve objectives.	Risk Assessment is the process of identifying and evaluating risks to understand their potential impact.
2.Objective	To provide a structured approach for managing uncertainties, reducing risks, and seizing opportunities.	To create a detailed understanding of risks, their likelihood, and their potential impact.

3.Scope	Broader, includes risk identification, assessment, prioritization, and treatment (mitigation or acceptance).	Narrower, focuses solely on identifying and evaluating risks. It is a part of risk management.

Q-02 .Inherent Risk vs. Residual Risk .BPE-6th.

Aspect	Inherent Risk	Residual Risk
1. Meaning	Inherent risk is the level of risk that exists before applying any controls or risk mitigation measures.	Residual risk is the level of risk that remains after controls and mitigation measures are applied.
2. Relation With Control	It exists without considering internal controls or risk management actions.	It exists after considering the effectiveness of internal controls.
3. Risk Level	Usually higher, as no control has yet reduced the risk.	Usually lower, because controls reduce the risk but cannot eliminate it fully.

Q-03. Quantitative Analysis vs. Qualitative Analysis . BPE-6th.

Aspect	Quantitative Analysis	Qualitative Analysis
1. Basis	Based on numerical data, ratios, and statistical models.	Based on judgment, experience, and descriptive assessment.
2. Type Of Factors	Deals with measurable factors such as financial ratios, probability, and loss amount.	Deals with non-measurable factors such as management quality, governance, and risk culture.
3. Nature Of Result	Results are objective and easily comparable.	Results are subjective but provide deeper understanding.

Q-04. How does it differ from the traditional silo-based approach to risk management? BPE-6th.

Aspect	ERM	Silo-Based Approach
1. Approach	Manages all risks in an integrated, organization-wide manner.	Manages risks separately by department.
2. Risk View	Takes a holistic view of total risk exposure.	Takes a partial view of risks.
3. Coordination	Ensures coordination among all units under a central framework.	Little or no coordination among units.

Chapter End