RMFI Questions 98th AIBB

Question No: 1

a) What is risk management? What is the relationship between risk management and capital management? (6 marks)

Risk Management

Risk management is the process of identifying, assessing, mitigating, and monitoring potential risks that could negatively impact an organization's financial health, operations, or reputation. In banking and financial institutions, risk management is crucial for ensuring stability and sustainability. It involves managing various types of risks, such as credit risk, market risk, operational risk, liquidity risk, and compliance risk.

A sound risk management framework helps organizations:

- Minimize financial losses
- Comply with regulatory requirements
- Improve decision-making processes
- Maintain investor and customer confidence
- Enhance business resilience

Relationship between Risk Management and Capital Management

Risk management and capital management are closely linked, as both aim to ensure a financial institution’s stability and long-term viability.

1. **Capital as a Buffer Against Risks**
    - Banks hold capital reserves to absorb unexpected losses arising from various risks.
    - A strong risk management strategy helps in determining the appropriate level of capital needed to mitigate these risks.
2. **Regulatory Requirements**
    - Regulatory frameworks like **Basel III** require banks to maintain minimum capital levels based on their risk exposure.
    - Effective risk management ensures compliance with capital adequacy requirements.
3. **Capital Allocation Efficiency**

- Risk management helps banks allocate capital efficiently by assessing the risk-return trade-off of different investments.
- Institutions can prioritize capital deployment to areas with controlled risks and higher returns.

4. **Mitigation of Financial Instability**
    - Poor risk management can lead to capital depletion due to unexpected losses.
    - A well-structured capital management strategy ensures that banks have enough capital to cover risks without negatively affecting operations.

Conclusion

Risk management and capital management work together to safeguard a bank's financial health. While risk management focuses on identifying and mitigating threats, capital management ensures that adequate financial resources are available to absorb potential losses. A strong integration of both practices enhances financial resilience, regulatory compliance, and overall business sustainability.

b) Briefly describe the elements of sound risk management system. (7 marks)

A well-structured risk management system is essential for financial institutions to identify, assess, and mitigate risks effectively. The key elements include:

1. **Risk Identification** – Recognizing potential risks that could impact the organization, such as credit, market, operational, and liquidity risks.
2. **Risk Assessment & Measurement** – Evaluating the likelihood and impact of identified risks using qualitative and quantitative methods.
3. **Risk Mitigation & Control** – Implementing policies, internal controls, and strategies to minimize or manage risks effectively.
4. **Risk Monitoring & Reporting** – Continuously tracking risk exposures and reporting them to senior management and regulators to ensure proactive decision-making.
5. **Governance & Oversight** – Establishing a strong risk culture with clear roles and responsibilities for the Board of Directors, Risk Committees, and Management.
6. **Regulatory Compliance** – Ensuring adherence to local and international risk management regulations, such as Basel III and central bank guidelines.

A sound risk management system enhances financial stability, regulatory compliance, and decision-making, helping organizations manage uncertainties effectively.

c) Define risk culture. Outline the effective strategies that financial institutions can implement to reinforce and enhance its risk culture. (7 marks)

Definition of Risk Culture

Risk culture refers to the shared values, attitudes, and behaviors within an organization that influence how risks are identified, assessed, and managed. A strong risk culture ensures that employees at all levels understand the importance of risk management and integrate it into their decision-making processes.

Effective Strategies to Reinforce and Enhance Risk Culture

1. **Leadership Commitment** – Senior management and the Board of Directors must lead by example, promoting a culture of accountability and transparency in risk management.
2. **Clear Risk Policies & Guidelines** – Establish well-defined risk policies, frameworks, and standard operating procedures to guide employees in risk-related decision-making.
3. **Risk Awareness & Training** – Conduct regular training and awareness programs to ensure employees understand risk principles and their role in managing risks.
4. **Open Communication & Reporting** – Encourage employees to report risks without fear of retaliation by fostering a transparent and open risk reporting environment.
5. **Integration with Performance Management** – Align risk management with performance evaluation by incorporating risk-related metrics into key performance indicators (KPIs).
6. **Independent Risk Oversight** – Maintain an independent risk management function that continuously monitors risk practices and provides unbiased assessments.
7. **Regular Stress Testing & Risk Assessments** – Implement periodic stress tests and scenario analyses to identify vulnerabilities and strengthen risk preparedness.
8. **Regulatory Compliance & Governance** – Ensure strict adherence to local and international regulatory requirements, reinforcing ethical risk-taking behaviors.

By adopting these strategies, financial institutions can build a strong risk culture that promotes resilience, minimizes losses, and supports sustainable growth.

Question No: 2

a) What is risk register? Discuss the components of a risk register. (7 marks)

Risk Register: **A** Risk Register **is** a structured document or database used in risk management to identify, assess, and track potential risks that may impact an organization. It serves as a centralized tool for recording risks, their potential impact, mitigation strategies, and responsible personnel. Financial institutions and businesses use risk registers to proactively manage and minimize risks.

Components of a Risk Register:

1. **Risk ID** – A unique identifier assigned to each risk for easy reference.
2. **Risk Description** – A brief explanation of the risk, including its nature and potential impact.
3. **Risk Category** – Classification of the risk (e.g., financial, operational, credit, compliance, market risk).
4. **Risk Likelihood** – An assessment of the probability of the risk occurring (e.g., low, medium, high).
5. **Risk Impact** – The potential severity of the risk on business operations or financial health.
6. **Risk Owner** – The individual or department responsible for monitoring and managing the risk.
7. **Risk Mitigation Measures** – Strategies and actions planned to minimize or eliminate the risk.
8. **Current Risk Status** – An update on whether the risk is active, mitigated, or resolved.
9. **Risk Rating** – A numerical or qualitative score based on likelihood and impact, helping prioritize risks.
10. **Review Date** – Scheduled date for reassessment to ensure continuous monitoring and control.

Conclusion: A well-maintained risk register helps organizations systematically manage risks, ensuring proactive decision-making and regulatory compliance. It enhances transparency, accountability, and overall risk resilience.

b) What are the Key Risk Indicators (KRI) for financial institutions? How do they differ from Key Performance Indicators (KPIs)? (7 marks)

Key Risk Indicators (KRIs) for Financial Institutions

Key Risk Indicators (KRIs) are measurable metrics that help financial institutions identify, assess, and monitor potential risks that could impact their operations, stability, and profitability. KRIs provides early warning signals to help organizations take proactive measures before risks escalate.

Common KRIs in Financial Institutions:

1. **Credit Risk KRIs**
    - Non-Performing Loan (NPL) ratio
    - Loan default rates
    - Borrower creditworthiness deterioration
2. **Market Risk KRIs**
    - Interest rate volatility
    - Foreign exchange fluctuations
    - Value at Risk (VaR) levels
3. **Liquidity Risk KRIs**
    - Loan-to-deposit ratio
    - Liquidity coverage ratio (LCR)
    - Unused credit lines and funding gaps
4. **Operational Risk KRIs**
    - Number of fraud incidents
    - System downtime or cyber security breaches
    - Regulatory fines and compliance breaches
5. **Reputational Risk KRIs**
    - Customer complaints and negative media coverage
    - Declining customer satisfaction scores
    - Employee turnover rates in key departments

Difference between KRIs and KPIs:

Aspect	Key Risk Indicators (KRIs)	Key Risk Indicators (KRIs)
Definition	Metrics used to monitor potential risks and threats.	Metrics used to monitor potential risks and threats.
Purpose	Helps in risk prevention and early warning detection.	Helps in risk prevention and early warning detection.
Focus	Identifies vulnerabilities and exposures.	Identifies vulnerabilities and exposures.
Examples	High NPL ratio, rising fraud cases, liquidity shortfall.	High NPL ratio, rising fraud cases, liquidity shortfall.
Outcome	Helps in mitigating risks and ensuring stability.	Helps in mitigating risks and ensuring stability.

c) Define risk rating? Analyze its pros and cons in risk management. (6 marks)

Definition of Risk Rating

Risk rating is a systematic approach used to assess and categorize risks based on their likelihood and potential impact on an organization. It helps financial institutions and businesses prioritize risks and allocate resources for mitigation accordingly. Risk ratings are typically expressed using numerical scales (e.g., 1-5) or qualitative categories (e.g., low, medium, high).

Pros of Risk Rating in Risk Management

- ✓ **Improved Decision-Making:** Helps organizations prioritize risks and allocate resources effectively.
- ✓ **Regulatory Compliance:** Ensures adherence to regulatory frameworks like Basel III, which require risk assessment.
- ✓ **Early Risk Identification:** Enables proactive risk mitigation by identifying threats before they escalate.
- ✓ **Enhanced Transparency:** Provides a structured method to communicate risk levels to stakeholders.
- ✓ **Better Capital Allocation:** Helps banks determine capital reserves needed to cover potential risks.

Cons of Risk Rating in Risk Management

✖ **Subjectivity:** Risk assessments may vary based on personal judgment, leading to inconsistencies.

✖ **Data Limitations:** Inaccurate or incomplete data can lead to incorrect risk categorization.

✖ **Static Nature:** Risk ratings may not always reflect rapid market or economic changes.

✖ **Over-Reliance on Models:** Excessive dependence on risk models may overlook emerging risks.

✖ **Complexity in Implementation:** Requires expertise, technology, and regular updates to remain effective.

Question No: 3

a))The Board of Directors (BoD) has the ultimate responsibility for the risk taken by the bank. Evaluate the statement. (7 marks)

The statement that the Board of Directors (BoD) has the ultimate responsibility for the risk taken by the bank is both accurate and fundamental to good corporate governance. As the highest governing body within a bank, the BoD holds the ultimate accountability for overseeing the bank's entire risk management strategy. This includes ensuring that appropriate structures, processes, and policies are in place to identify, assess, and manage a wide range of risks the bank may encounter, such as credit, market, liquidity, operational, and reputational risks.

While management is responsible for the day-to-day implementation of the bank's risk management framework, the BoD is tasked with establishing the overall strategic direction of the bank's risk profile. This includes approving the risk appetite, setting the risk limits, and ensuring that management aligns its decisions with the bank's risk tolerance and regulatory requirements. In addition, the BoD must ensure that adequate resources are allocated for effective risk management, including the establishment of independent risk oversight functions such as a Chief Risk Officer (CRO).

The BoD is also responsible for monitoring risk exposure at a high level, reviewing risk reports, and ensuring that the risk management process is integrated into the bank’s overall operations. Furthermore, the BoD must make certain that the bank complies with both local and international regulatory requirements, such as Basel III, and that risk management is continuously evolving in response to changing economic conditions, market dynamics, and emerging risks.

Ultimately, the BoD is accountable to shareholders, regulators, and other stakeholders for the bank's risk-taking activities. A failure in risk governance at the BoD level can have severe consequences, potentially leading to financial instability, legal penalties, and damage to the bank's reputation. Therefore, the responsibility of managing and overseeing the risks taken by the bank rests squarely with the BoD, making it critical for them to remain proactive, well-informed, and engaged in the bank’s risk management activities.

b) What are the minimum criteria for appointing a Chief Risk Officer (CRO) as per Bangladesh Bank guidelines? (6 Marks)

According to the Bangladesh Bank guidelines, the **Chief Risk Officer (CRO)** must meet certain minimum criteria to ensure that they have the necessary expertise and experience to effectively manage and oversee the bank's risk management framework. These criteria include the following:

1. **Educational Qualifications**: The CRO should have at least a graduate degree in fields such as finance, economics, business administration, or other related disciplines. Advanced degrees (such as an MBA or relevant professional certifications) are considered an added advantage.
2. **Professional Experience**: The CRO should have a significant amount of experience in risk management or related fields. Typically, this would include at least 10 years of professional experience in financial services, with a substantial portion of that time spent in roles directly related to risk management.
3. **Knowledge and Expertise**: The CRO must possess a comprehensive understanding of various types of risks (such as credit, market, operational, and liquidity risks) and risk management techniques. Additionally, the individual should be well-versed in Bangladesh's banking regulations, risk assessment practices, and international risk management standards like Basel III.
4. **Independence and Objectivity**: The CRO should be in a position to perform their duties independently and objectively, without any conflict of interest. This is essential to ensure the integrity of risk assessments and decision-making processes.
5. **Reporting Structure**: The CRO should report directly to the Board of Directors (BoD) or the Board Risk Management Committee (BRMC), ensuring the independence of risk management activities and the proper oversight of the risk management function.
6. **Ethical Standards**: The CRO should adhere to high ethical standards and demonstrate strong leadership and decision-making capabilities. They should also foster a strong **risk culture** within the bank and be able to communicate effectively with senior management and the BoD.

7. **Regulatory Compliance**: The CRO should be able to ensure that the bank complies with Bangladesh Bank's risk management guidelines and other regulatory frameworks, including Basel standards and other local regulatory requirements.

By fulfilling these criteria, the CRO can effectively oversee the bank's risk management function, helping to maintain financial stability and ensure the bank's long-term sustainability.

c) "Audit Committee and Internal-Auditors are considered as an extension of the Board Risk Management Committee (BRMC)" - Do you agree with statement? Justify your answer. (7 Marks)

Yes, I agree with the statement that the **Audit Committee** and **Internal Auditors** are considered as an extension of the **Board Risk Management Committee (BRMC)**. Here's why:

The **Board Risk Management Committee (BRMC)** is responsible for overseeing the risk management framework within a bank, ensuring that risks are adequately identified, assessed, and mitigated. The BRMC's role is to provide strategic direction on risk management and ensure compliance with regulatory requirements.

Role of Audit Committee and Internal Auditors in Risk Management

1. **Audit Committee**:

   The Audit Committee plays a critical role in overseeing the effectiveness of the bank's internal controls and risk management systems. It works closely with the BRMC to evaluate whether the risk management processes are functioning as intended. The Audit Committee's responsibilities often include reviewing risk-related reports, monitoring the effectiveness of internal controls, and ensuring that financial statements reflect a true and fair view of the bank's risk exposure. Therefore, the Audit Committee's work supports the BRMC's risk management activities, providing oversight and helping ensure that risk management practices are aligned with the bank's strategy and regulatory requirements.

2. **Internal Auditors**:

   Internal auditors assess the adequacy of the risk management framework and internal controls. They independently evaluate the effectiveness of risk mitigation measures and identify areas of concern. Internal auditors provide the BRMC with detailed reports on risk management practices, ensuring that any weaknesses or gaps are addressed promptly. By performing regular audits of the bank's risk management systems and controls, internal auditors offer the BRMC objective insights into how risks are being handled and whether the risk management policies are being adhered to.

Justification of the Statement

Both the Audit Committee and Internal Auditors provide critical support and ensure that the risk management activities overseen by the BRMC are functioning effectively. They help ensure that risk management is not just a theoretical framework but is being implemented with operational rigor and integrity. Since these entities evaluate the robustness of risk controls and ensure compliance with regulations, they act as an extension of the BRMC by enhancing its oversight and accountability functions.

Moreover, internal auditors and the Audit Committee are not directly involved in risk-taking activities, which allows them to maintain an independent perspective and serve as an objective check on the risk management processes. This independence and their detailed risk assessments complement the BRMC's role in setting the overall risk strategy and risk appetite.

Conclusion

In conclusion, the Audit Committee and Internal Auditors indeed function as extensions of the BRMC because they provide independent oversight, evaluation, and assurance that risk management activities are appropriately implemented and effective. Their role supports the BRMC’s mission of ensuring comprehensive and effective risk governance within the bank.

Question No: 4

a) If you are an employee of Risk Management Division then under which stage of 3 lines of Defense (3LoD) you are working? Write the prime responsibilities of this stage. (7 Marks)

If I were an employee of the **Risk Management Division**, I would be working under the **second line of defense (2LoD)** in the **Three Lines of Defense (3LoD) model**.

Explanation of the Second Line of Defense (2LoD):

In the 3LoD model, the **second line of defense** is responsible for overseeing and supporting the first line of defense (which is the operational management) in identifying, assessing, and mitigating risks. This line is typically made up of risk management, compliance, and other control functions that provide an additional layer of defense and independent assurance that the risk management processes are operating effectively.

Prime Responsibilities of the Second Line of Defense (Risk Management Division):

1. **Risk Management Framework Implementation**:
    - The second line is responsible for developing, implementing, and maintaining the bank's risk management framework. This includes setting policies, processes, and methodologies for identifying, assessing, and managing various types of risks (credit, market, operational, liquidity, etc.).
2. **Risk Oversight and Monitoring**:
    - The Risk Management Division ensures that risk exposures are monitored regularly. They conduct risk assessments, stress testing, and scenario analysis to evaluate the bank's risk profile and the adequacy of risk controls.
3. **Risk Reporting**:
    - The second line is responsible for reporting on risk exposures to the Board of Directors (BoD) and senior management. This includes providing insights into risk trends, risk mitigation actions, and any emerging risks that may require attention.

4. **Providing Expertise and Guidance**:
    - Risk management professionals in the second line offer expertise and guidance to the first line of defense (operational management). They assist business units in managing risks by providing tools, techniques, and advice on how to handle specific risk issues.
5. **Compliance and Regulatory Adherence**:
    - The second line ensures that risk management processes align with regulatory requirements and industry standards (such as Basel III). They support the business in staying compliant with internal policies and external regulations.
6. **Independent Risk Assessment**:
    - While the first line of defense handles day-to-day operations, the second line provides an independent assessment of the risks identified and the effectiveness of mitigation strategies. They act as a check to ensure that the operational management is not underestimating or overlooking potential risks.
7. **Risk Control and Mitigation Strategy**:
    - The second line helps design and implements effective risk control measures and mitigation strategies. They work with the first line to ensure that controls are functioning as intended and recommend changes if necessary.

b)"Operational risk is common in all activities of a bank" – Do you agree with this statement? Justify your opinion. (7 Marks)

Yes, I agree with the statement that "operational risk is common in all activities of a bank." Operational risk refers to the possibility of loss due to inadequate or failed internal processes, human error, system failures, or external events. This type of risk is inherent in every aspect of a bank's operations, as banks perform a wide variety of activities that require complex systems, processes, and human involvement. For example, in lending, errors can occur in processing loan applications or in communication with customers, leading to potential financial losses. Similarly, trading activities are at risk due to system failures, erroneous trades, or mistakes made by employees.

Banks are heavily dependent on technology for many of their functions, such as electronic payments, online banking, and data processing. Any failure in these technological systems, whether through cyber-attacks, system outages, or software bugs, can introduce significant operational risk. For instance, a failure in an ATM network or an online banking platform can disrupt services and result in both financial losses and reputational damage.

Human error is another critical factor that contributes to operational risk in banks. Mistakes made by employees—such as incorrect data entry, failure to follow procedures, or poor decision-making—can lead to financial losses or disruption of operations. Even in the case of regulatory compliance, operational risk arises from failure to meet regulatory requirements. If banks fail to comply with rules such as anti-money laundering laws or capital adequacy standards, they could face legal penalties and damage to their reputation.

Additionally, operational risks can also stem from external events such as natural disasters, political instability, or terrorism. These events can cause significant disruptions to a bank’s operations, particularly if the systems or processes are not designed to handle such situations.

Even though banks implement risk management systems to mitigate operational risks, these systems are not perfect. Failures in internal controls, lapses in risk management frameworks, or misalignment of risk policies can still result in unforeseen operational issues. Therefore, it is accurate to say that operational risk is common to all activities in a bank, and it is essential for banks to integrate effective risk management strategies to manage this risk.

c) What are the challenges faced by banks in managing operational risk in Bangladesh? (6 Marks)

Banks in Bangladesh face several challenges in managing operational risk due to a combination of internal and external factors.

- **Inadequate infrastructure and outdated technology**: Many banks in Bangladesh rely on old systems that are vulnerable to cyber-attacks, system failures, and technological disruptions.
- **Lack of skilled professionals**: There is a shortage of experienced risk management professionals, which hampers the ability to effectively identify, assess, and mitigate operational risks.
- **Human error**: Operational risks arising from manual processes are common, leading to mistakes in transactions and other banking activities.
- **Compliance challenges**: The regulatory environment is constantly evolving, and banks face difficulties in staying up to date with compliance requirements, making it harder to manage operational risk.
- **External factors**: Events such as natural disasters, political instability, and economic fluctuations disrupt banking operations, particularly in rural and underdeveloped areas.
- **Insufficient risk culture and awareness**: A lack of awareness and strong risk culture within banks leads to poor implementation of risk management practices, increasing the likelihood of operational risks.

Question No: 5

a) Discuss different steps involved in successful implementation of ERM. (7 Marks)

The successful implementation of **Enterprise Risk Management (ERM)** involves several critical steps to ensure that risks are identified, assessed, mitigated, and monitored effectively across the organization. Below are the key steps involved:

1. **Establishing Risk Management Framework**: The first step in implementing ERM is to develop a comprehensive risk management framework. This includes defining the organization's risk appetite, risk tolerance, and overall risk management objectives. The framework should also outline the processes, roles, and responsibilities for risk management within the organization.
2. **Risk Identification**: A critical step is identifying potential risks that could affect the organization. This involves reviewing both internal and external factors, such as market conditions, regulatory changes, technological risks, and operational challenges. Engaging stakeholders across the organization ensures that a wide range of risks is considered.
3. **Risk Assessment and Analysis**: Once risks are identified, they need to be assessed in terms of their likelihood and potential impact. This is done through qualitative and quantitative analysis. Tools such as risk matrices or probability-impact charts can help in evaluating and prioritizing the risks based on their significance to the organization.
4. **Risk Mitigation and Control**: After assessing the risks, the next step is to develop strategies to mitigate or control them. This may involve implementing internal controls, adopting risk avoidance strategies, transferring risks through insurance, or accepting certain risks if they fall within the organization’s risk tolerance.
5. **Developing and Implementing Policies**: Clear policies and procedures must be established to guide the implementation of risk management strategies. This includes setting guidelines for decision-making, risk-taking activities, and control measures. Training employees and stakeholders on these policies is also essential for ensuring alignment.
6. **Monitoring and Reporting**: Continuous monitoring of risks is essential to ensure that mitigation strategies are effective and that new risks are identified promptly. Regular

reporting of risk management activities to senior management and the board helps keep them informed and ensures accountability.

7. **Review and Improvement**: ERM should be a dynamic process that is reviewed regularly. The effectiveness of the risk management framework and mitigation strategies should be assessed and improvements should be made based on lessons learned, changes in the business environment, or emerging risks. This helps keep the risk management system responsive to changing circumstances.

In conclusion, the successful implementation of ERM requires a structured approach, starting with a strong framework, followed by identification, assessment, and mitigation of risks, and continuous monitoring and improvement. This ensures that risks are managed in a way that aligns with the organization's objectives and long-term success.

b) What is stress testing? Explain its significance in risk management. (8 Marks)

Stress testing is a risk management technique used to assess how certain stress scenarios or adverse conditions could impact an organization, particularly its financial stability and overall risk exposure. It involves simulating extreme but plausible adverse events or shocks, such as economic downturns, market crashes, or regulatory changes, to evaluate how these events would affect the organization's assets, liabilities, and overall performance.

Significance in Risk Management:

1. **Identifying Vulnerabilities**: Stress testing helps identify potential vulnerabilities in the organization's risk profile. By simulating extreme scenarios, such as a severe market decline or a credit crisis, banks and financial institutions can pinpoint areas where they may be exposed to higher risk, such as liquidity issues or asset value declines.
2. **Improving Capital Planning**: Stress tests help in assessing the adequacy of the institution's capital reserves. By understanding how the organization would perform under stress conditions, it can adjust its capital buffers and ensure it has sufficient funds to withstand adverse events.
3. **Regulatory Compliance**: Regulatory bodies, such as central banks, often require financial institutions to perform stress tests to ensure that they can remain solvent and maintain financial stability during periods of economic stress. Meeting these regulatory requirements demonstrates the organization's ability to manage risks effectively.
4. **Enhancing Risk Management Strategies**: The results of stress testing provide valuable insights into potential risks that may not be apparent under normal conditions. This enables banks and institutions to adjust their risk management strategies, such as tightening credit policies, improving liquidity management, or diversifying investments, to better handle potential shocks.
5. **Scenario Planning**: Stress testing supports scenario analysis by providing a structured way to model potential future risks. It helps organizations prepare for unlikely but high-impact events, ensuring they are better equipped to manage unexpected situations and continue their operations.

6. **Improving Decision-Making**: By simulating different stress scenarios, stress testing informs decision-making at senior management and board levels. It helps in prioritizing risk mitigation actions, deciding on risk appetite levels, and making informed strategic decisions related to financial stability and growth.

In conclusion, stress testing is a critical tool in risk management as it helps organizations anticipate and plan for extreme but possible risks, ensuring that they can withstand financial shocks and continue operating smoothly in challenging environments.

c) Compare SWOT and PESTLE analysis as risk assessment technique. (5 Marks)

SWOT and **PESTLE** analyses are two widely used risk assessment techniques, each serving different purposes in evaluating risks within an organization. Below is a comparison of the two:

1. SWOT Analysis

Definition: SWOT stands for **Strengths, Weaknesses, Opportunities,** and **Threats**. It is a strategic planning tool used to identify internal and external factors that could impact an organization's objectives and performance.

Focus:

- **Internal Factors**: Strengths and Weaknesses focus on the internal environment of the organization.
- **External Factors**: Opportunities and Threats focus on the external environment, such as market trends, competition, and external risks.

Key Features:

- **Strengths**: Internal capabilities that give the organization an advantage in achieving its goals.
- **Weaknesses**: Internal limitations that hinder the organization's ability to achieve its goals.
- **Opportunities**: External factors that the organization can leverage to enhance its performance.
- **Threats**: External factors that could harm the organization's performance or objectives.

Usefulness:

- Helps in understanding the **current position** of an organization.
- Identifies **key internal weaknesses** and external threats.
- Facilitates **strategic decision-making** by focusing on both internal and external factors.

Limitations:

- It is a **static analysis** that may not fully account for changes in the external environment over time.
- Relies heavily on subjective assessments, which may lead to **bias** in identifying risks.

2. PESTLE Analysis

Definition: PESTLE stands for **Political, Economic, Social, Technological, Legal,** and **Environmental** factors. It is a tool used to analyze and monitor the macro-environmental factors that could influence an organization's performance.

Focus:

- **External Factors Only**: PESTLE focuses exclusively on the external environment, offering a broader perspective of the factors that can impact the organization.

Key Features:

- **Political**: Refers to government policies, political stability, and regulations affecting the organization.
- **Economic**: Economic factors, such as inflation rates, exchange rates, and economic growth that could influence the business environment.
- **Social**: Demographic and cultural factors that could affect consumer behavior and market demand.
- **Technological**: Technological advancements or disruptions that could impact operations, products, or services.
- **Legal**: Laws, regulations, and legal challenges that affect the industry or market.
- **Environmental**: Environmental factors like climate change, sustainability regulations, and natural disasters that can impact operations.

Usefulness:

- Provides a **holistic view** of the external environment.
- Helps in **anticipating long-term trends** and emerging risks, allowing organizations to adapt.
- Useful for organizations operating in diverse geographical regions, as it identifies local and global external factors.

Limitations:

- Does not focus on internal factors, so it may overlook risks arising from the organization's internal processes, structures, or strategies.
- Requires frequent updates as the external environment is dynamic and ever-changing.

Comparison:

- **Scope**: SWOT evaluates both internal and external factors, whereas PESTLE focuses solely on external environmental factors.
- **Application**: SWOT is more **organization-centric** and used for assessing immediate risks and opportunities, while PESTLE is broader, helping organizations understand how macro-environmental factors could affect their future performance.
- **Focus**: SWOT helps identify **specific risks** related to strengths, weaknesses, opportunities, and threats, while PESTLE offers a **broader view** of external trends and risks that may affect the organization in the long term.
- **Nature of Analysis**: SWOT is more **static** and often used for **short-term** analysis, while PESTLE helps assess **long-term trends** that may impact the organization's strategic direction.

Conclusion:

Both SWOT and PESTLE analyses are valuable tools in risk assessment, but they serve different purposes. SWOT provides an organization with insights into both internal capabilities and external threats, which is useful for immediate and operational risk assessment. PESTLE, on the other hand, offers a more comprehensive view of the external environment, helping organizations anticipate long-term macroeconomic and societal risks. Ideally, both techniques should be used together to offer a complete risk assessment framework.

Question No: 6

a) What is ALCO? How is it constituted? (5 Marks)

ALCO stands for **Asset and Liability Committee**. It is a senior management committee within financial institutions (such as banks) that is responsible for overseeing the management of assets and liabilities to ensure financial stability, liquidity, and profitability. The primary objective of ALCO is to manage financial risks associated with liquidity, interest rates, and the overall balance sheet structure.

Constitution of ALCO: ALCO is typically composed of senior executives from different areas of the bank, such as:

- **Chief Financial Officer (CFO)**: Often serves as the chairperson of the committee.
- **Treasury Head**: Responsible for managing liquidity and capital.
- **Risk Management Head**: Oversees risk-related issues.
- **Chief Economist**: Provides insights into economic factors affecting financial strategies.
- **Senior Executives**: Including members from other departments such as operations, audit, and compliance.

The committee meets regularly to review financial strategies, assess market risks, and make decisions related to managing interest rate risk, liquidity risk, and capital adequacy.

b) What are the functional differences among front, mind and back office of treasury? (8 Marks)

The **front office**, **middle office**, and **back office** in the treasury of a financial institution have distinct roles in managing financial transactions, risks, and operations.

1. **Front Office**:

The front office is responsible for the **execution of transactions** and direct market-facing activities. Its functions include:

- **Trading**: Engaging in buying and selling of financial instruments such as bonds, stocks, and derivatives.
- **Sales**: Engaging with clients to sell financial products.
- **Risk Management**: Managing the day-to-day market risk exposures arising from trading activities.

The front office is crucial for generating profits by taking calculated market positions and managing client relationships.

2. **Middle Office**:

The middle office acts as a **risk management and compliance** function, bridging the gap between the front office and back office. Its functions include:

- **Risk Monitoring**: Monitoring the risks associated with trading and investment activities executed by the front office.
- **Valuation**: Ensuring the correct valuation of trades, portfolios, and financial instruments.
- **Compliance and Reporting**: Ensuring that all transactions are compliant with regulatory requirements and internal policies.

The middle office focuses on ensuring that the front office's activities are aligned with the institution's risk appetite and regulatory framework.

3. **Back Office**:

The back office is responsible for the **settlement and administrative support** of transactions. Its functions include:

- **Trade Settlements**: Ensuring the proper execution and settlement of trades, including the transfer of funds and securities.
- **Record Keeping**: Maintaining accurate records of all transactions and positions.
- **Reconciliation**: Ensuring that the financial records are consistent across all departments and systems.
- **Accounting and Reporting**: Preparing financial statements and reports based on the trades and transactions.

The back office ensures the smooth processing and accurate reporting of financial transactions, ensuring operational efficiency.

c) What is the market risk? Explain the sources of market risk in the financial institution. (7 Marks)

Market risk refers to the potential for financial losses due to changes in the market conditions that can impact the value of an institution's assets, liabilities, or positions. These changes may arise from fluctuations in interest rates, stock prices, commodity prices, or foreign exchange rates. Market risk is a crucial factor that financial institutions must manage to protect their profitability and financial stability.

Sources of Market Risk in Financial Institutions:

1. **Interest Rate Risk**:
    - **Definition**: The risk of loss due to fluctuations in interest rates that affect the value of financial instruments, such as loans, bonds, and derivatives.
    - **Impact**: An increase in interest rates can reduce the market value of fixed-income securities and affect the institution's profitability on variable-rate loans.
2. **Equity Price Risk**:
    - **Definition**: The risk of loss arising from changes in the prices of stocks and equity investments.
    - **Impact**: A decline in stock market prices could lead to a reduction in the value of equity holdings, affecting financial institutions holding significant equity positions.
3. **Foreign Exchange Risk**:
    - **Definition**: The risk associated with fluctuations in exchange rates between currencies.
    - **Impact**: Institutions that engage in foreign currency trading or hold foreign-denominated assets and liabilities are exposed to the risk of adverse currency movements, which can lead to financial losses.
4. **Commodity Price Risk**:
    - **Definition**: The risk arising from fluctuations in the prices of commodities such as oil, metals, or agricultural products.

- **Impact**: Financial institutions involved in commodity trading or holding commodity-linked assets may experience volatility due to changes in commodity prices, impacting their portfolios.

5. **Liquidity Risk**:
    - **Definition**: The risk that an institution may not be able to meet its short-term financial obligations due to changes in market conditions or the inability to convert assets into cash quickly.
    - **Impact**: A disruption in market liquidity can affect the institution's ability to sell assets or raise capital, increasing the potential for market risk.

In conclusion, market risk is a significant concern for financial institutions, and it is influenced by various factors such as interest rates, equity prices, foreign exchange fluctuations, commodity prices, and liquidity conditions. Effective risk management practices are essential to mitigate market risk and ensure financial stability.

Question No: 7

a) What is ICT risk management? How does cyber security risk differ from ICT risk? Explain. (7 Marks)

ICT Risk Management refers to the process of identifying, assessing, and mitigating risks related to Information and Communication Technology (ICT) systems and infrastructure within an organization. It focuses on the security, availability, and integrity of ICT systems, networks, hardware, and data. The goal is to ensure that the organization's technology resources and digital operations are protected from potential threats, disruptions, or failures that could negatively impact business continuity, data integrity, and the achievement of organizational objectives.

Key Differences between Cybersecurity Risk and ICT Risk:

- **Focus Area**: Cybersecurity risk focuses specifically on protecting digital information, networks, and systems from malicious cyber threats, while ICT risk covers all technology-related risks, including both cyber and non-cyber aspects (e.g., system failures, operational risks).
- **Scope**: Cybersecurity risk is a subset of ICT risk, as ICT risk includes not only cyber security threats but also other operational risks related to technology.
- **Mitigation**: Cybersecurity risk management primarily addresses measures to prevent cyber-attacks, while ICT risk management encompasses a wider range of strategies, including securing physical hardware, ensuring system continuity, and preventing technical failures.

(b) The Washington-based think tank, Global Financial Integrity (GFI), reported in December 2021 that Bangladesh loses an average of 8.27 billion USD annually due to mis-invoicing of imported and exported goods to evade taxes and illegally transfer money across international borders.
-Evaluate this statement based on the concepts of over-invoicing and under-invoicing. (7 Marks)

The statement by **Global Financial Integrity (GFI)** about Bangladesh losing **8.27 billion USD** annually due to mis-invoicing can be evaluated through the concepts of **over-invoicing** and **under-invoicing**.

- **Over-Invoicing** occurs when the price of goods is inflated on invoices, allowing individuals or companies to transfer more money abroad than the actual value of the goods. This helps evade taxes, customs duties, and facilitates illegal money transfers out of the country.
- **Under-Invoicing** involves declaring a lower value for goods, which reduces the customs duties and taxes owed, while allowing exporters to retain more foreign currency abroad.

Both practices lead to **tax evasion**, **capital flight**, and **money laundering**, depriving the government of revenue and draining foreign currency reserves.

Thus, the **8.27 billion USD** loss reflects the financial impact of these illicit activities, which harm Bangladesh's economy by reducing government income and promoting illegal financial outflows.

(c) Mention at least ten (10) important indicators of poor credit risk management. (6 Marks)

Here are ten important indicators of poor credit risk management:

1. **High Default Rates**: A significant number of loans or credit products going into default are a clear sign of poor credit risk management.
2. **Inadequate Credit Assessment**: Failure to properly assess borrowers' creditworthiness, such as insufficient background checks or reliance on outdated information.
3. **Concentration Risk**: Excessive exposure to a single borrower, sector, or geographical region, making the portfolio vulnerable to sector-specific downturns.
4. **Weak Monitoring and Reporting**: Lack of regular monitoring of outstanding loans and inadequate reporting systems to track repayment schedules or early signs of distress.
5. **Lack of Diversification**: A portfolio heavily concentrated in high-risk loans or sectors with little diversification increases the potential for significant losses.
6. **Non-Compliance with Regulatory Standards**: Failure to comply with regulatory requirements on loan provisioning, credit limits, and risk-weighted asset calculations.
7. **Inadequate Risk Mitigation Strategies**: Absence of effective measures, such as collateral or credit derivatives, to protect against defaults.
8. **Weak Loan Recovery Process**: Delayed or ineffective efforts to recover non-performing loans, resulting in higher write-offs.
9. **Excessive Credit Extensions**: Granting credit to borrowers without considering their ability to repay or extending loans in inappropriate economic conditions.
10. **Low Credit Rating Quality**: Having a significant proportion of loans with low credit ratings, indicating a higher likelihood of defaults and financial instability.

Question No: 8

a) Discuss the capital requirements for banks as per the Basel-III capital guidelines of Bangladesh Bank. *(8 Marks)*

Basel-III, introduced by the **Bank for International Settlements (BIS)**, sets more stringent capital and liquidity requirements to strengthen the global banking system. Bangladesh Bank, in line with Basel-III, has established specific capital requirements to improve the resilience of financial institutions.

1. **Tier 1 Capital (Core Capital)**:
    - Banks are required to maintain a minimum **4.5%** of their **Risk-Weighted Assets (RWA)** in Tier 1 capital. This is the core capital, consisting primarily of **common equity**, and is the most reliable capital in absorbing losses.
2. **Tier 2 Capital**:
    - Banks must have a minimum **2.0%** of their RWA in Tier 2 capital, which includes **subordinated debt** and other instruments that can absorb losses in the event of bank failure but are less permanent than Tier 1 capital.
3. **Capital Conservation Buffer**:
    - In addition to Tier 1 and Tier 2, Basel-III requires banks to maintain a **2.5% capital conservation buffer** above the minimum capital requirements, aimed at ensuring banks have additional capital during economic downturns.
4. **Leverage Ratio**:
    - A **3%** minimum leverage ratio is required to prevent banks from taking excessive leverage. This ratio is defined as the ratio of Tier 1 capital to the bank's total exposure (including off-balance-sheet items).
5. **Systemically Important Banks**:
    - For **domestic systemically important banks (D-SIBs)**, additional capital requirements are imposed to reduce the risk of systemic collapse.

These capital requirements ensure that banks are better able to absorb losses during financial stress, reducing the likelihood of a systemic crisis.

b) Why is liquidity important in banking? Which pillar of Basel-III discusses liquidity risk? (7 Marks)

Why is Liquidity Important in Banking?

Liquidity is crucial for banks because it ensures they can meet their **short-term obligations** and continue their operations smoothly. Here are some key reasons:

1. **Operational Continuity**: Banks must have enough liquidity to conduct day-to-day operations, such as processing withdrawals, granting loans, and settling debts. Without sufficient liquidity, a bank could face disruptions, potentially leading to a liquidity crisis.
2. **Market Confidence**: Liquidity is essential for maintaining **customer and investor confidence**. If a bank cannot fulfill its financial obligations, it could face a loss of trust, leading to a run on the bank or a sharp decline in its stock value.
3. **Risk Mitigation**: Liquidity buffers help banks handle unexpected situations, like **market shocks** or **economic downturns**, without needing to rely on risky or short-term funding.

Which Pillar of Basel-III Discusses Liquidity Risk?

Liquidity risk is addressed under **Pillar 2** of **Basel-III**, which is the **Supervisory Review Process**. Basel-III requires banks to assess and manage liquidity risks as part of their internal risk management frameworks, even though liquidity risk is not fully covered by the minimum capital requirements set in **Pillar 1**.

Basel-III also introduces specific liquidity standards under **Pillar 1**, including:

1. **Liquidity Coverage Ratio (LCR)**: Requires banks to maintain an adequate stock of high-quality liquid assets (HQLA) to cover net cash outflows for a 30-day stress period.
2. **Net Stable Funding Ratio (NSFR)**: Requires banks to ensure they have stable funding for a longer-term horizon (one year), minimizing reliance on short-term funding.

Together, these requirements ensure that banks maintain liquidity buffers, helping them survive periods of financial stress.

c) How does the adaptation of the Basel-III capital accord improve risk management in financial institutions? (5 Marks)

The adaptation of Basel-III improves risk management in financial institutions in several ways:

1. **Stronger Capital Base**: Basel-III requires higher levels of high-quality capital (Tier 1), ensuring that banks have a stronger financial cushion to absorb losses during economic shocks, reducing systemic risk.
2. **Enhanced Liquidity Standards**: With the introduction of the Liquidity Coverage Ratio (LCR) and the Net Stable Funding Ratio (NSFR), Basel-III ensures banks maintain sufficient liquidity to survive stress scenarios, thereby minimizing the risk of liquidity crises.
3. **Leverage Control**: The introduction of the leverage ratio limits the amount of borrowing relative to capital, preventing banks from excessive risk-taking through high leverage and reducing the likelihood of financial instability.
4. **Risk Sensitivity**: Basel-III encourages banks to align their capital with the risks they face (through risk-weighted assets), ensuring that risk management practices are more tailored and dynamic.
5. **Systemic Risk Mitigation**: By addressing issues related to systemically important banks (D-SIBs), Basel-III reduces the risk of the failure of large institutions having an outsized impact on the global financial system.

Overall, Basel-III enhances the resilience of financial institutions, improves the quality of capital, and ensures more robust liquidity management, leading to a safer banking environment.

Q9. Case Study: SVB Fallout

Silicon Valley Bank (SVB) was the largest bank by deposits in Silicon Valley due to its specialized services for tech investors. In 2022, SVB began incurring steep losses following increased interest rates and a major downturn in the tech industry. The bank was heavily concentrated in long-term treasury bonds. As of December 31, 2022, SVB had mark to market accounting unrealized losses exceeding $15 billion for securities held to maturity.

Regulatory filings from December 2022 estimated that more than 85% of deposits were uninsured. SVB was without a Chief Risk Officer (CRO) for about eight months in 2022. Additionally, regulatory standards for SVB were too low, and supervision was not conducted with sufficient force and urgency. In March 2023, after the central bank endorsed an interest rate hike, there was a bank run on its deposits, leading to its collapse. The failure of SVB was the largest of any bank since the 2007–2008 financial crises by assets and the second largest in US history, behind the collapse of Washington Mutual.

Based on the information above and other published data, answer the following questions: **(4 × 5 = 20 Marks)**

(a) Discuss the key reasons for the SVB fallout.

(b) Explain the specific role of the Board of Directors (BoD) in the SVB fallout.

(c) Briefly explain the risks faced by SVB that led to its collapse.

(d) Were there any risk management control functions in place that could have mitigated the overall impact of the risk?

(e) If proper risk management and corporate governance had been in place, the collapse of SVB would not have happened. Evaluate this statement from the perspective of a risk manager.

(a) Key Reasons for the SVB Fallout

Several key factors contributed to the collapse of Silicon Valley Bank (SVB):

1. **Interest Rate Hikes**: In 2022, the Federal Reserve increased interest rates to combat inflation. SVB had a significant concentration in **long-term treasury bonds**, which saw their value decline as interest rates rose. The **unrealized losses** from these bonds exceeded $15 billion by the end of the year, severely damaging the bank's balance sheet.
2. **Concentration in the Tech Sector**: SVB's business model was heavily reliant on tech startups and venture capital. The downturn in the tech industry led to **higher deposit withdrawals**, as startups burned through cash reserves to survive, while investments in the tech sector suffered.
3. **Uninsured Deposits**: Over **85% of SVB's deposits** were uninsured. When the bank's financial situation worsened, the lack of FDIC insurance for such a large portion of deposits led to a **run on the bank** as depositors rushed to withdraw their funds.
4. **Absence of a Chief Risk Officer (CRO)**: SVB was without a CRO for about **eight months in 2022**, which left a significant gap in its risk management framework. This absence likely contributed to inadequate monitoring of risks and delayed response to the evolving crisis.
5. **Regulatory Failures**: Regulatory standards for SVB were too **lenient**, and there was insufficient supervision of the bank’s risks. This lack of oversight failed to highlight the growing risks until it was too late.

(b) Specific Role of the Board of Directors (BoD) in the SVB Fallout

The **Board of Directors (BoD)** of SVB played a crucial role in the bank's collapse by failing in several key areas:

1. **Risk Oversight**: The BoD was responsible for overseeing the bank's risk management framework. The **absence of a CRO** should have been flagged as a major governance issue, but the BoD did not take timely action to fill this gap.
2. **Failure to Diversify**: The BoD allowed SVB to concentrate its exposure in the tech sector and long-term treasury bonds, which left the bank vulnerable to interest rate hikes and a downturn in the tech industry.
3. **Inadequate Crisis Management**: As the bank's financial situation deteriorated, the BoD did not implement sufficient measures to shore up confidence or mitigate the risks. The BoD failed to manage liquidity risks effectively during the critical period leading to the run on the bank.
4. **Regulatory Compliance**: The BoD also failed to push for higher regulatory standards and better supervision, which contributed to the bank's exposure to risks without sufficient checks.

(c) Risks Faced by SVB That Led to Its Collapse

SVB faced several risks that ultimately led to its downfall:

1. **Interest Rate Risk**: The bank's concentration in **long-term treasury bonds** exposed it to significant interest rate risk. As rates rose, the value of these bonds fell, leading to massive **unrealized losses**.
2. **Concentration Risk**: SVB's business was overly reliant on the **tech industry** and **venture capital firms**, which suffered a downturn in 2022. This left the bank vulnerable when tech startups began to withdraw deposits to cover operational costs.
3. **Liquidity Risk**: SVB lacked sufficient **liquidity buffers**. The heavy reliance on uninsured deposits, combined with the bank's liquidity mismatches (e.g., long-term securities against short-term deposit withdrawals), led to a **bank run** in March 2023.
4. **Credit Risk**: SVB was exposed to credit risk through its lending to startups and venture-backed firms, which, during a downturn in the tech industry, faced higher failure rates and credit stress.
5. **Operational Risk**: The absence of a **Chief Risk Officer (CRO)** for a prolonged period created an operational gap in risk management and risk mitigation strategies, contributing to the bank's inability to address escalating risks in time.

(d) Risk Management Control Functions That Could Have Mitigated the Overall Impact of the Risk

There were several risk management controls that could have potentially mitigated the impact of the crisis:

1. **Effective Liquidity Management**: SVB could have maintained more **diversified liquid assets** to withstand deposit withdrawals, reducing the risk of a bank run. More effective stress-testing of liquidity positions could have identified vulnerabilities earlier.
2. **Active Risk Monitoring**: The absence of a **CRO** left the bank vulnerable to rapid changes in risk exposure. A dedicated risk officer would have implemented stronger **risk monitoring frameworks** to assess interest rate risks, sector concentration, and other vulnerabilities on an ongoing basis.
3. **Diversification of Assets**: A more diversified asset portfolio, reducing exposure to **long-term treasury bonds** and the **tech sector**, could have helped SVB better weather interest rate hikes and industry downturns.
4. **Stronger Internal Controls**: Robust internal controls to assess and manage credit, market, and operational risks could have reduced the chances of significant losses. More proactive **regulatory compliance** and risk assessment could have highlighted the growing risks and prompted corrective action.

(e) Evaluation of the Statement: "If Proper Risk Management and Corporate Governance Had Been in Place, the Collapse of SVB Would Not Have Happened"

From a **risk manager's perspective**, the statement holds significant validity:

1. **Risk Identification and Mitigation**: If SVB had a strong **risk management framework** in place, the **interest rate risk** and **liquidity risk** would have been more effectively identified and mitigated. A **Chief Risk Officer (CRO)** could have helped ensure the bank was prepared for changes in interest rates, providing proactive solutions like hedging or rebalancing its portfolio.
2. **Diversification**: Proper **diversification** of assets and deposits would have shielded the bank from the adverse effects of a concentrated position in treasury bonds and the tech sector. A more balanced portfolio could have reduced exposure to the specific risks that caused the crisis.
3. **Crisis Management**: **Corporate governance** would have prompted the BoD to take more aggressive actions in times of distress, like strengthening liquidity buffers, diversifying income streams, and enhancing the bank's crisis management strategies.
4. **Regulatory Compliance**: Stronger adherence to **regulatory standards** would have ensured that the bank was under more effective supervision and was held to higher standards of risk management, possibly preventing some of the risk-taking behavior that led to the collapse.

In conclusion, proper risk management and corporate governance would have enabled SVB to better anticipate and mitigate the risks that led to its downfall, potentially preventing the crisis or minimizing its impact.

10. Write short notes on any five of the following: (5 × 5 = 25 Marks)

(a) Contingency Planning

(b) Leverage Ratio (LR)

(c) Board Risk Management Committee (BRMC)

(d) Risk Appetite

(e) Settlement Risk

(f) Environmental & Social (E&S) Risk Management

(g) Market Discipline

(a) Contingency Planning

Contingency planning is a proactive process of preparing for potential future events that could disrupt normal operations. It involves identifying risks, developing response strategies, and implementing measures to ensure business continuity. In banking, contingency planning covers areas such as liquidity crises, cyber-security breaches, and operational disruptions. A well-structured contingency plan helps financial institutions minimize losses and restore operations quickly in case of emergencies.

(b) Leverage Ratio (LR)

Leverage Ratio (LR) measures a bank's financial leverage by comparing its core capital to its total assets, including off-balance-sheet exposures. It is a key indicator of a bank’s ability to absorb losses and maintain financial stability. Under Basel-III, banks must maintain a minimum leverage ratio to prevent excessive borrowing and reduce systemic risks. A higher leverage ratio indicates lower risk, while a lower ratio may suggest higher financial vulnerability.

(c) Board Risk Management Committee (BRMC)

The Board Risk Management Committee (BRMC) is a specialized committee within a bank's board of directors responsible for overseeing risk management policies, frameworks, and strategies. Its main duties include:

- Identifying and assessing key risks, including credit, market, liquidity, and operational risks.
- Ensuring compliance with regulatory requirements and internal risk policies.
- Reviewing and approving risk management frameworks to align with business objectives.
- Reporting significant risk exposures to the Board of Directors for necessary actions.

(d) Risk Appetite

Risk appetite defines the level of risk an organization is willing to accept in pursuit of its strategic goals. It is influenced by factors such as capital adequacy, regulatory requirements, and market conditions. Financial institutions establish risk appetite statements that guide decision-making across different risk categories, including credit risk, liquidity risk, and operational risk. A well-defined risk appetite ensures that the bank operates within acceptable risk limits while achieving growth objectives.

(e) Settlement Risk

Settlement risk arises when one party in a financial transaction fails to fulfill its obligations after the other party has already delivered its commitment. It is common in foreign exchange, securities trading, and interbank transactions. This risk can occur due to technical failures, counterparty insolvency, or regulatory restrictions. Measures to mitigate settlement risk include using real-time gross settlement (RTGS) systems, central clearinghouses, and legally binding contractual agreements.

(f) Environmental & Social (E&S) Risk Management

Environmental and Social (E&S) Risk Management refers to the process of identifying, assessing, and mitigating risks associated with environmental and social factors in financial decision-making. Banks and financial institutions integrate E&S risk management to ensure that lending and investment activities do not harm the environment or society. Key aspects include:

- Assessing the environmental impact of financed projects.
- Ensuring compliance with sustainability regulations and ESG (Environmental, Social, and Governance) standards.
- Avoiding reputational risks related to financing unethical or unsustainable projects.

(g) Market Discipline

Market discipline is a regulatory framework under Basel-III that promotes transparency and accountability in financial institutions. It requires banks to disclose key financial and risk-related information to the public, enabling investors, customers, and regulators to assess their financial health and risk exposure. Market discipline helps prevent excessive risk-taking by ensuring that stakeholders can make informed decisions based on publicly available data.