Republic of the Union of Myanmar

Central Bank of Myanmar

Guideline on Risk Management Practices of Banks

6th Waxing of Tazaungmon 1382 ME

20th , November, 2020

1. In the exercise of its powers under Section 184 of the Financial Institutions Law (FIL), the Central Bank of Myanmar (CBM) hereby issues the following Guideline.

Title and Application

2. This Guideline shall be called the Guideline on Risk Management Practices of Banks.

3. This Guideline applies to all banks.

Definitions

4. Terms used in this Guideline have the following meanings:

(a) Risk means the probability of a material financial loss to the bank due to exposure to, and uncertainty arising from, current and potential future events. Seven types of key financial risk (credit, market, liquidity etc.) are defined in Annexe; 1 to 7 to the Guideline.

(b) Risk management system means the overall framework adopted by the Board of Directors for managing the bank's risks, including its risk appetite, policies and procedures for identifying, measuring, monitoring and managing risk and the governance of its risk management decisions.

(c) Risk appetite framework has the meaning set out in paragraph 24 of this Guideline.

(d) Stress test shall mean an analysis conducted by the bank on the impact of an unfavourable scenario such as a recession, financial market crisis or of a change in a variable such as an exchange rate, designed to determine whether the bank has adequate capital and/or liquidity to withstand the impact of adverse developments.

(e) Senior management means the officers of the bank responsible for the management of the bank on a day–to–day basis, including the chief executive as defined in Section 2 of the FIL, chief financial officer and chief risk management officer.

(f) Officer shall have the meaning set out in Section 2 of the FIL.

(g) Independent Non–Executive director shall have the meaning set out in the CBM Directive on Directors of Banks (No. 9/2019).

Objectives

5. All banks assume risks in the normal course of their business. If they are not adequately managed, such risks may lead to significant loss, eroding profitability and capital resources and ultimately putting the bank's depositors' funds at risk and endangering financial stability. Banks therefore need to establish a comprehensive risk management system, overseen by the bank's Board of Directors, to identify, measure, monitor and control their risks. Stress testing should be used to evaluate the bank's

vulnerability to certain severe but plausible events or movements in financial variables such as interest or exchange rates. The risk management system should include management of banks' risks related to money laundering and the financing of terrorism.

6. The FIL sets out requirements on risk management, including:

(a) Section 74 (c) (1) and (2) establish the responsibilities of the Board of Directors which include adopting and reviewing a comprehensive risk management process; and establishing and reviewing the system and procedures of control and risk management.

(b) Section 58 sets out requirements in relation to credit facilities, including for adequate internal policies, practices and procedures.

(c) Under Section 96 (a) (13) the CBM may require a bank to enhance its governance, internal controls and risk management systems.

7. The CBM's Directive on Directors of Banks (No. 9/2019) sets out further requirements on Boards of Directors which include establishing the bank's risk appetite and overseeing the bank's adherence to its risk policy and risk limits.

8. Section 28 of the Anti–money Laundering Law 2014 sets out requirements on the adoption, development and implementation of internal programs, policies, procedures and controls for managing

effectively and mitigating risks related to money laundering. The CBM's Guidance Note on AML/CFT Risk Based Management, issued on 27 January 2015, sets out the CBM's expectations on how banks manage their money laundering/terrorist financing risks. The CBM's Directive on Customer Due Diligence related to the Anti-money Laundering and Counter Financing of Terrorism (Directive No. 18/2019), issued 15 November, 2019, set out more detailed requirements.

9. The objectives of this Guideline are:

(a) to set out the CBM's requirement on risk management that banks ensure that their risk management system is appropriate to the nature, scale and complexity of their business;

(b) to encourage banks to enhance their risk management practices, taking into account developments in the financial system in Myanmar and the bank's strategy and plans for the development of its business; and

(c) to set out the standards which the CBM uses in assessing risk management systems under its risk-based approach to supervision.

10. The CBM's key standards are set out in this Guideline. More detailed standards on risk management for key types of financial risk are set out in Annexes; 1 to 7. The CBM will in due course issue separate detailed guidelines on stress testing by banks.

The Risk Management System

11. Banks should ensure that their risk management system includes:

(a) **A system of comprehensive risk identification:** in order to manage risks, a bank should be able to recognize and understand all its material risks, including those arising from proposed new business initiatives. Banks should be able to identify: Risk identification should be a continuing process and should include risks across the portfolio as well as by customer and transaction.

(i) all material inherent risks in each activity or business line (for example, in relation to lending business, the liquidity, interest rate and operational risks in addition to credit risks); and

(ii) for each type of risk, all relevant activities (for example, credit risk in trade finance and foreign exchange business as well as loans);

(b) **Risk measurement methodologies:** once identified, risks should be measured using appropriate techniques, accurately and on a timely basis, to determine their potential impact on the bank's financial position. Banks should regularly test their risk measurement tools to ensure they provide accurate measurements on a portfolio basis as well as by customer, transaction etc.

(c) **Risk Monitoring:** banks should establish management information systems to monitor risk and facilitate timely review of risk positions and any exceptions, taking account of the bank's risk appetite. Monitoring reports should be frequent, timely, accurate and informative and should be made available to the senior management and Board of Directors to ensure action, when needed.

(d) **Risk Control:** banks should have appropriate controls over risk, including limits and tools for mitigating risk. Banks should maintain policies and procedures that define responsibilities and authorities for risk management. They should have a process to authorize and document exceptions or changes to risk limits.

12. Banks' risk management systems should include the management of money laundering and financing of terrorism risks. Banks should ensure that they understand the risks present in their customer base, products, delivery channels and services and the jurisdictions where they and their customers do business. Policies and procedures for customer acceptance, due diligence and on–going monitoring should be designed and implemented to adequately control their identified risks. The CBM's Directive on Customer Due Diligence related to the Anti–money Laundering and Counter Financing of Terrorism (Directive No. 18/2019) and Guidance Note on AML/CFT Risk Based Management, issued 27 January 2015, set out more detailed requirements.

Risk Governance: Board oversight

13. Consistent with their responsibilities for risk management under Section 74 (c) (1) and (2) of the FIL and paragraph 12 of the CBM's Directive (9/2019) on Directors of Banks, Boards of Directors should:

(a) approve the bank's risk appetite framework and a comprehensive risk strategy setting out, for example, the types and amounts of risk which the bank will accept consistent with its business strategy;

(b) approve the risk management system, taking into account the bank's risk appetite, risk strategy, business plan and risk policies and senior management's capacity to manage its activities; and approve the bank's risk policies and procedures;

(c) ensure that senior management is taking the necessary steps to identify, measure, monitor, and control the bank's risks and is otherwise implementing risk policies, procedures and controls effectively; and

(d) receive reports that identify the size and significance of the risks in terms that can be used by the Board to assess the development of the bank's risks in relation to risk appetite and to decide on actions.

14. Board members should receive regular training from time to time. Banks should put in place a continuous professional development program to ensure that directors are equipped with the appropriate skills and

knowledge to perform their roles, including as members of Board committees, effectively. Such programs may include a detailed overview and risk profile of the institution’s significant or new business lines and periodic updates on regulatory developments. Risks related to money laundering and financing of terrorism should be included in the program.

15. Under Section 75 of the FIL, the Board of Directors may form one or more committees or sub–committees for specific purposes, including a Risk Management Committee. Boards of Directors should consider the benefits in relation to creating an effective risk management system. The CBM expects Boards of Directors, especially of large banks, to establish such a committee. The Risk Committee should be chaired by an Independent Non–Executive director of the bank.

16. In some cases, it will be appropriate for the Board of Directors to delegate risk management matters to its Audit Committee, as a responsibility additional to those set out Section 85 of the FIL. Arrangements should be established for reporting on risk management by the relevant Board committees to the Board of Directors, which shall retain overall responsibility for the risk management of the bank.

Risk Governance: Responsibilities of Senior Management

17. Senior management is responsible for implementing the bank’s risk management system. Senior management should ensure that risk policies and procedures agreed by the Board as well as the Board–approved risk appetite framework are:

(a) transformed into operational policies, procedures and processes for effective day–to–day risk management;

(b) communicated effectively within the bank and supported by appropriate staff training as well as measures to promote the awareness of risk and the importance of effective risk management at all levels of the bank; and

(c) implemented effectively throughout the bank, with significant exceptions (such as breaches of limits) identified, reported and addressed with appropriate actions.

18. Senior management should be aware of the bank's risk profile on a continuing basis and ensure that the Board of Directors and its Risk Management Committee or Audit Committee, as applicable, are informed of the development of the bank's risks in relation to risk appetite. They should implement Board–approved changes to the risk appetite framework and risk policies and procedures.

19. Members of senior management should be fully aware of and understand the activities undertaken by the bank that could expose it to risk. They should have sufficient knowledge and skills to manage risks in line with the board's risk appetite.

20. Boards of Directors and senior management should appoint an officer of the bank to be responsible as chief risk management officer for the management of the bank's overall, bank-wide risks. The chief risk management officer should have responsibility for the bank's risk management function, as described in this Guideline, and should attend meetings of the Board of Directors to report on developments in the risks of the bank.

Risk Governance: The Risk Management Function

21. Banks should establish a function to be responsible to the senior management for overall, bank-wide risk management. The function should be independent from those units and staff which take or accept risk for the bank, including the bank's business units. Where individuals responsible for overall bank-wide risk management are also involved in day to day operations, controls should be established to ensure that effective, independent risk management is not adversely affected.

22. The risk management function should have responsibility for providing an oversight of the management of the risks inherent in the bank's activities. The duties of the function should include:

(a) identifying current and emerging risks, including those related to money laundering and the financing of terrorism;

(b) developing risk assessment and risk measurement systems;

(c) establishing (and supporting business units to establish) policies, practices and other control mechanisms to manage risks;

(d) developing the bank's risk appetite and related framework of limits for senior management and Board of Directors approval;

(e) monitoring positions against approved risk limits; and

(f) reporting results of risk monitoring to the senior management, the Board of Directors and relevant committees of the Board.

23. While the risk management function is responsible for bank-wide risk management, the officers responsible for the management of business units have the best understanding of the risks in their activities and should be responsible for their risks. They should cooperate with the risk management function in the development of policies and procedures on risk identification, risk measurement, monitoring and control and in the effective implementation of the risk management system.

Risk Appetite Framework

24. Banks should establish an appetite for the aggregate level and types of risk they are willing to assume, decided in advance and within their risk capacity, to achieve their strategic objectives and business plan. Banks should include risks which they seek to take in order to generate returns (including credit, market and liquidity risks) and risks which arise in the course of the business (such as operational and reputational risks).

25. The bank's risk appetite framework may be defined using measures such as:

(a) a target credit rating for the bank, where applicable;

(b) the amount of change in the profit or loss which the bank is prepared to accept;

(c) the maximum impact on capital adequacy (as measured by the ratio of capital to risk–weighted assets) or on the level of liquidity which the bank wants to hold, to ensure it can meet its minimum regulatory requirements under normal and stressed conditions.

26. The bank's risk appetite should be kept under review by the bank's senior management and risk management function and reviewed by the Board of Directors at least annually.

Adequate Policies and Procedures

27. The Board of Directors and senior management should develop and implement risk management policies and procedures to address the bank's risks. The bank's policies and its detailed procedures should provide guidance for the day–to–day implementation of risk management objectives. For each risk, they should include:

(a) the sources of risk that the bank is willing to take, consistent with its risk appetite framework;

(b) the bank's approach to measurement of risk, including key risk measurement tools, assumptions, data sources, and the approach to aggregation of risk measures across activities and across risks;

(c) procedures for monitoring risk and reporting risk levels and exceptions to senior management and the Board of Directors;

(d) accountability and lines of authority in the bank's business units;

(e) the role and responsibility of the risk management function, risk committees (including the Risk Management Committee or Audit Committee of the Board, as applicable) and of the Board of Directors;

(f) policies and procedures on risk mitigation, including the bank's policy on the management of collateral and other forms of security, hedging transactions etc.;

(g) procedures for establishing controls over risk, including risk limits, and the role of internal audit in relation to the bank's risks;

(h) procedures for assessing risk in relation to new products and new business lines.

28. The bank's policies and procedures should include risks related to money laundering and financing of terrorism. They should cover policies on risk assessment of customers and transactions, identification and verification of the customer, application of customer due diligence measures to customers, on–going customer due diligence measures and enhanced due diligence measures for high risk customers. More detailed requirements are set out in the Directive on Customer Due Diligence related to the Anti–money Laundering and Counter Financing of Terrorism (Directive No.18/2019).

29. The Board of Directors should review risk policies, procedures, and limits regularly and ensure that they are updated by the management of business units and by the risk management function when necessary. Revised risk policies and procedures should be agreed by the Board of Directors.

30. Risk policies and the procedures used in measuring, monitoring and controlling risk should be appropriately documented. Documentation should be kept under review by the management of business units and by the risk management function and updated regularly or as policies and procedures change.

Adequate Risk Monitoring and Management Information Systems

31. The Board of Directors and senior management should ensure that there are effective systems to enable the bank to monitor its material risks and respond to risk developments as necessary.

32. The bank’s approach to risk monitoring should be supported by management information systems (MIS) that capture relevant information accurately and on a timely basis, aggregate it appropriately and generate comprehensive reports for risk managers, senior management and the Board of Directors. The reports for staff engaged in the day–to–day management of the bank's activities should be sufficiently detailed to enable them to manage risks effectively. Reports for senior management and the Board of Directors should highlight key developments, divergence from risk appetite, key trends in risk exposure and new and emerging risks.

33. Risk reporting should include environmental developments, such as movements in interest rates, currencies, market prices of securities etc. and key macroeconomic developments, assessing how these affect the risks of the bank.

34. The risk monitoring system should enable risk managers, including the risk management function to identify breaches in risk limits and to propose appropriate actions in response.

Adequate Internal Controls, including internal audit

35. Banks should establish effective controls over risk as a part of their risk management system. Key controls include:

(a) the establishment and implementation of a comprehensive framework of limits covering all the banks' risks, together with systems and procedures to enforce limits effectively;

(b) an internal organization, defined responsibilities and reporting lines that together provide for separation of risk taking from risk management and control, including: independence of the risk management function from business units and separation of duties relating to the granting of credit and credit control, trading and settlement, setting and monitoring of limits etc;

(c) procedures to identify and respond to new risks, including risks related to new products or customers and macroeconomic and other environmental risks; and

(d) comprehensive documentation of risk policies and procedures and of the risk decisions taken by the bank.

36. In addition, internal controls over risk should be evaluated and tested as appropriate, by an independent internal auditor who reports directly either to the bank's Board of Directors or to its Audit Committee. The internal auditor should be asked to report on appropriate matters, including:

(a) whether the risk management system is functioning effectively, enabling the bank to identify, measure, monitor and control risks in accordance with risk appetite and established risk management policies and procedures;

(b) the integrity of the bank’s risk management information system, including the accuracy and completeness of data used in risk measurement and monitoring;

(c) whether breaches in risk limits are being identified and reported in a timely manner and whether action is being taken in response to such breaches and exceptions in accordance with the bank’s policies and procedures;

(d) whether accountabilities and responsibilities for risk management, including the separation of duties and the independence of the risk management function, are operating effectively and in accordance with the Board–approved procedures;

(e) the adequacy of the bank’s documentation of its risk management policies and procedures and records of key decisions;

(f) whether previously identified material weaknesses in controls have been addressed appropriately and on a timely basis; actions taken by management in response to such material weaknesses should be verified and reviewed.

37. The bank's Audit Committee and Board of Directors should review the findings of internal audit on the risk management system at least annually.

Stress Testing

38. Banks should develop and implement a rigorous and well–documented stress testing framework that is proportionate to the scale, nature and complexity of their operations and appropriate to their material risks. Stress tests should be undertaken on a regular basis. Stress testing should contribute to banks’ risk identification, measurement and monitoring. Banks should use stress tests in their decision–taking.

39. While the CBM may mandate certain stress tests or the minimum frequency and scope of stress testing and require banks to report their stress tests results, banks are responsible for the design and conduct of stress tests and for taking appropriate action in response to the stress test results.

40. Detailed requirements on stress testing will be set out in a separate Guideline to be issued by the CBM.

External Audit

41. Requirements on external audit are set out in Chapter XI of the FIL and in the CBM's Directive on External Auditors of Banks (No. 10/2019). The Board of Directors, Audit Committee and senior management of the bank should ensure that where issues have been raised by the bank's external auditors in relation to the risk management system, including relevant controls, these issues are addressed, and appropriate action taken. Such issues have been raised in the external auditors' audit report, the management letter or another report connected with the audit or may have arisen in meetings between the bank, its external auditors and the CBM.

Capital Management Plan

42. Banks should establish capital management plans to ensure that the bank's available capital is, and will remain, commensurate with the level of the bank's risks as well as sufficient to meet its business objectives and to comply with capital adequacy requirements set out in the FIL and by the CBM, including the Capital Adequacy Regulation (CAR) (Notification No. 16/2017).

43. In assessing capital needs in relation to risks, banks should take account of all their risks, including those not subject to the CBM's capital requirements. They should assess likely future capital demands and their ability to raise new capital, if required. Capital management plans should take into account the bank's policy on payment of dividends to shareholders.

44. Banks' capital management plans should be approved by the Board of Directors.

Supervision by the Central Bank of Myanmar

45. Under Section 93 of the FIL, the CBM has the responsibility and duty to monitor the performance of banks to ensure their compliance with all applicable standards. To help the CBM to meet this responsibility, it is adopting a risk–based approach to the supervision of banks, which takes account of banks' risk management practices. The CBM expects banks:

(a) to be able to explain in detail their risk management system, including how they ensure compliance with the requirements of the FIL, CBM Directives and this Guideline; banks may be asked at any time to submit copies of the documentation of their risk management system, including their risk management policies and procedures, as well as internal risk reports and internal audit reports on risk management;

(b) to discuss the operation of their risk management system in practice at meetings with CBM supervisors, including in the course of inspections under Section 91 of the FIL; these discussions may include detailed questions on the bank's policies and practices;

(c) to account for how their risks have been developing and may develop further in the future, with reference to recent decisions on risk; banks may be asked to submit copies of internal risk reports, including risk reports to the Board of Directors or Risk Management Committee, where applicable.

46. Banks should keep the CBM informed of significant changes in their risk management system, including changes in risk appetite and risk strategy and key changes in risk policies and procedures. They should submit all new or significantly revised documentation to the CBM with an explanation of the nature and reasons for the change.

47. In addition to existing regular reports on the balance sheet, income statement etc., the CBM may require banks to submit statistical and other information on their risks.

Non–Compliance with this Guideline

48. Failure to comply with this Guideline constitutes a violation and is subject to corrective actions or sanctions as may be imposed under Section 94 and 96 of the FIL and administrative penalties under Section 154.

Effectiveness

49. This Guideline shall come into effect 6 months from the issued date.

Withdrawal of CBM Directive on Credit Risk Management

50. The CBM's Directive for Credit Risk Management (No. 4/2017) is withdrawn and replaced by this Guideline on the date on which this Guideline takes effect.

Sd./xxxxxxx

For Governor

BO BO Nge, Deputy Governor

ANNEX 1: Credit Risk

Credit risk is the risk of loss resulting from the failure of a borrower to meets its obligations under a credit facility granted by the bank or from a reduction in the value of the bank's assets due to a change in the credit quality of the borrower/counterparty.

1. Banks should identify all sources of material credit risk in their business, including in their lending, trade finance, treasury and foreign exchange operations as well as credit risk in their investments, other assets and in their off–balance sheet business.

2. Banks should measure all their material credit risk, adopting appropriate measurement techniques. They should:

   (a) develop tools and techniques (which may include estimates of probability of default, loss given default etc. as well as information from credit bureaux and expert judgment) to assess and to assign credit quality ratings to individual credits;

   (b) have tools specifically to assess the credit risk on new loans before deciding whether and on what terms (including pricing) to grant credit, based primarily on the borrower's financial strength and capacity to repay;

   (c) use current market prices and credit ratings, where available, to measure:

      (i) credit risk in investments, identifying credit spreads; and

(ii) counterparty and settlement risks in foreign exchange, treasury business etc.;

(d) be able to distinguish between loans that are performing and likely to remain so and those which are deteriorating and those which have become non–performing;

(e) account for loans and other credit facilities in accordance with accounting standards;

(f) maintain tools to measure credit risk across the portfolio, including the use of:

(i) measures of concentration risk (individual borrowers, sectors, countries);

(ii) stress tests to make a forward–looking assessment of potential future credit risk (see separate Guideline to be issued by the CBM).

3. Banks should <u>monitor</u> their material credit risks. They should:

(a) regularly review individual credits, evaluating financial information and holding discussions with management as appropriate;

(b) ensure that collateral is revalued on a regular basis and additional amounts required, where possible, in response to shortfalls;

(c) monitor changes in credit ratings and credit spreads on investment portfolios;

(d) maintain procedures for addressing delinquent credits, including referrals to a specialist unit responsible for managing such credits;

(e) establish provisions against delinquent and non–performing loans in line with the CBM’s Directive on Asset Classification and Provisioning (No. 17/2017);

(f) ensure that management information systems (MIS) capture information on the bank’s credit risks that is accurate and regularly updated; the MIS should be able to aggregate different types of exposure to the same counterparty and groups of connected counterparties and all exposures to individual economic sectors etc.;

(g) make regular reports on credit risk, including portfolio risk, to the credit committee, senior management, Risk Management Committee and Board of Directors.

4. Banks should <u>control</u> all material credit risk in their business. They should:

(a) establish, and monitor compliance with a Board–approved risk appetite and strategy for credit risk, covering all types and sources of credit risk;

(b) establish and monitor compliance with limits, including on exposures to:

(i) activities or products, such as the share of overdraft lending in the portfolio and exposures arising from off–balance sheet products;

(ii) single counterparties and groups of connected counterparties, including other banks and financial institutions, domestic and foreign;

(iii) specific economic sectors and geographic regions, including other countries;

(iv) types of collateral;

(v) related parties;

(vi) credit that is granted by individual managers approving credit facilities.

(c) establish techniques for mitigating credit risks such as taking of different forms of collateral (including but not limited to property), guarantees etc.;

(d) establish levels of authority for approving credit, including the responsibilities of a credit committee; and for other credit decisions including loan disbursements, foreclosures in case of failure to repay and write–off of irrecoverable loans;

(e) maintain procedures for managing delinquent credits, including remedial actions to restore loans to performing status (such as restructuring, rescheduling or changes to interest rates etc;) and for recognition of irrecoverable loans, including write–offs;

(f) ensure segregation of duties such as credit assessment, approval, disbursement, administration; and separation of the management of performing loans from the specialist unit responsible for managing delinquent credits;

(g) establish within the risk management function reporting to the chief risk management officer a credit risk unit or person responsible for bank–wide credit risk;

(h) establish processes for ensuring that the credit risk in new products and activities are assessed and that the risk falls within the bank's risk appetite;

(i) ensure that there is adequate documentation of all credit facilities, collateral arrangements etc. and that legal advice is taken on enforceability if necessary;

(j) undertake regular internal audit work on the effectiveness of controls over credit risk.

5. Banks should document their policies and procedures on credit risk, covering the types of credit they are prepared to grant, their procedures for identification, measurement, monitoring and control of credit risk; and for asset classification and provisioning. Banks' policies should be approved by the Board of Directors and implemented by senior management. They should include policies and controls for credit transactions with related parties, ensuring they comply with the requirements of the CBM's Related Parties Directive (No. 11/2019).

ANNEX 2: Market risk

Market risk is the risk to a bank resulting from adverse movements in market prices, in particular changes in interest rates, foreign exchange rates, equity (and other securities) and commodity prices.

1. Banks should <u>identify</u> all sources of material market risk in their business, including in foreign exchange trading and other foreign currency business (deposits and loans/other assets and liabilities denominated in foreign currencies), in their holdings (and trading) of marketable securities and commodities, if any. They should also identify their exposures to interest rate risk in their banking business and to the market risk that may arise in case of counterparty default in their derivatives business, if any, and in the settlement of purchases and sales of foreign currencies and investments.

2. Banks should <u>measure</u> their material market risk, adopting appropriate measurement tools and techniques. They should:

   (a) measure their exposure to foreign exchange risk, using measures that include the net open position, by currency and across all currencies;

   (b) measure their exposure to movements in prices of marketable securities, including equities, bonds and commodities, taking into account short positions (if any); they should calculate exposure and potential loss in case of assumed market movements;

(c) measure their exposure to changes in interest rates, using maturity mismatch analysis and applying assumed changes in interest rates (taking into account the CBM's requirements on interest rates); they should do so for MMK and significant foreign currencies separately; banks should measure exposure to risks arising from:

(i) mismatches in the timing of repricing of assets and liabilities and off–balance sheet positions (repricing risk);

(ii) changes in the slope and the shape of the yield curve (yield curve risk);

(iii) exposures that are hedged with exposure to a rate repricing under different conditions (basis risk);

(iv) options, if any; and

(v) fees and other income sensitive to changes in interest rates.

(d) measure concentrations of risk in the portfolio, for example exposures to multiple instruments that may react in the same manner to a specific market event; and measure concentrations in their gross risk as well as the net position;

(e) use appropriate quantitative techniques, such as Value–at–Risk, to identify and measure market risk;

(f) use stress tests to make a forward–looking assessment of potential future market risk (see separate Guideline to be issued by the CBM).

3. Banks should <u>monitor</u> their material market risks. They should:

(a) regularly review their market risk exposures to assess the development of the risk profile, including risk concentrations, and need for changes in their risk appetite;

(b) consider the establishment of an Asset and Liability Management Committee, either of the Board of Directors or senior management, responsible for monitoring and managing the bank's exposures to market risk;

(c) establish policies and procedures for managing market risk through hedging transactions, including the use of derivatives;

(d) ensure that management information systems (MIS) capture information on the bank's market risks that is accurate and regularly updated; their MIS should be able to aggregate exposure to market risks across the bank's activities;

(e) make regular reports on market risk to senior management, Board Risk Committee (and Asset and Liability Management Committee, if applicable) and to the Board.

4. Banks should <u>control</u> all material market risk in their business. They should:

(a) establish, and monitor compliance with a Board–approved risk appetite and strategy for market risk, covering all types and sources of market risk;

(b) establish and monitor compliance with limits on market risk, including limits on exposures to movements in exchange rates and interest rates, prices of marketable securities, commodities (where relevant); limits should apply to the aggregate exposure across the bank and to exposures in significant activities; separate limits may be appropriate for intraday exposures, as applicable;

(c) establish policy and procedures for the valuation of market risk exposures, including:

  (i) the choice of exchange and interest rates and market prices of securities used in measuring and monitoring risk; current market prices should be used, as determined by staff independent of those responsible for the exposures;

  (ii) the frequency of revaluations;

(d) establish the roles and responsibilities of the different functions of the bank for market risk and the levels of authority for approving market risk; they should in particular define the scope of responsibilities of the bank's treasury function;

(e) ensure the segregation of duties such as trading, valuation, risk management and confirmations/settlement;

(f) establish within the risk management function reporting to the chief risk management officer a market risk unit or person responsible for bank–wide market risk;

(g) establish processes for ensuring that new products and activities are assessed for market risk and that the risk falls within the bank's risk appetite;

(h) undertake regular internal audit work on the effectiveness of market risk controls.

5. Banks should document their policies and procedures on market risk, covering the types of risk they are prepared to take, their procedures for identification, measurement, monitoring and control of market risk and the decision–making authorities. Banks' policies should be approved by the Board of Directors and implemented by senior management.

ANNEX 3: Liquidity risk

Liquidity risk is the risk that the bank will be unable to meet expected and unexpected cash flow needs.

1. Banks should <u>identify</u> all sources of material liquidity risk, including risks arising from:

   (a) mismatches between the maturity of assets and liabilities;

   (b) limited access to high quality liquid assets such as actively traded government securities;

   (c) high reliance on short term interbank (or other wholesale) funding or a small number of large deposits;

   (d) participation in the payments system, including intra–day liquidity risks; and

   (e) liquidity demands from unfunded liabilities such as guarantees, committed but undrawn loans etc.

2. Banks should <u>measure</u> all their material liquidity risk, adopting appropriate measurement techniques. They should use:

   (a) appropriate ratios measuring the relationship between liquid assets, discounted where necessary to reflect limited market liquidity, and measures of liabilities;

   (b) maturity mismatch/gap analysis, calculated on both a contractual and behavioural basis, with appropriate assumptions (taking account of experience) about expected rollovers of demand and savings deposits, drawdown of loans etc.;

(c) cash flow projections showing likely net funding requirements over a short period;

(d) measures of liquidity risk by significant foreign currency;

(e) stress tests to make a forward–looking assessment of potential future liquidity risk, in particular the impact of net outflows in stress conditions (see separate Guideline to be issued by the CBM); the stress tests should include both stresses affecting only the bank and market–wide stresses and illiquidity in financial markets;

(f) measures of concentration risk (for example, large individual deposits or dependence on wholesale, including interbank, funding);

(g) early warnings indicators of liquidity risk such as a rapid growth in the bank's assets, funding concentrations, unexpected deposit outflows, significantly increased cost of funds, increased foreign currency business; a deterioration in asset quality; and negative publicity about the bank.

3. Banks should <u>monitor</u> their material liquidity risks. They should:

(a) regularly review their liquidity risks to assess the development of the risk profile, including risk concentrations, and any need for changes in their risk appetite;

(b) consider the establishment of an Asset and Liability Management Committee to be responsible for monitoring and managing the bank's liquidity;

(c) regularly test market access (for example by activating borrowing facilities from other banks);

(d) assess the extent of the assets which are available for use as collateral (such as government securities) against borrowing from other banks or the Central Bank;

(e) ensure that management information systems (MIS) capture information on the bank's liquidity that is accurate and regularly updated; banks' MIS should be able to aggregate liquidity across different activities, including off–balance sheet business;

(f) make regular reports on liquidity to the Assets and Liability Management Committee (if applicable), senior management, Board Risk Committee and Board of directors.

4. Banks should <u>control</u> all material liquidity risk in their business. They should:

(a) establish, and monitor compliance with a Board–approved risk appetite and strategy for liquidity risk, covering all types and sources of liquidity risk;

(b) establish and monitor compliance with limits on liquidity risk, including limits on:

(i) gaps between the maturities of assets and liabilities at appropriate intervals/maturity buckets; and

(ii) liquidity risk concentrations, both for liabilities and assets;

(c) establish techniques and policies for mitigating liquidity risks such as increasing time deposits or longer term interbank funding, negotiating committed liquidity facilities from other banks and increasing holdings of liquid assets;

(d) establish the roles and responsibilities of the different functions of the bank for liquidity risk and the levels of authority for approving risk; they should define the scope of responsibilities of the bank's treasury function;

(e) establish within the risk management function reporting to the chief risk management officer a liquidity risk unit or person responsible for bank–wide liquidity risk;

(f) establish processes for ensuring that new products and activities are assessed for their liquidity risk and that they fall within the bank's risk appetite;

(g) develop a comprehensive, realistic funding plan for addressing funding requirements in case of a liquidity stress, including:

(i) measures to address the funding profile, including seeking longer maturity deposits and arrangements to borrow from other banks;

(ii) measures to improve net cash flow related to the bank's assets such as suspension of loan disbursements/ rollovers, calling in overdrafts etc;

(iii) measures in relation to liquid assets such as conservation of those assets that may be used as collateral in interbank or CBM borrowing;

(iv) specific measures in relation to foreign currency funding;

(h) undertake regular internal audit work on the effectiveness of liquidity risk controls.

5. Banks should document their policies and procedures on liquidity risk, covering their risk appetite, their procedures for identification, measurement, monitoring and control of liquidity risk; decision–making authorities; their contingency funding plans; and internal controls. Banks' policies should be approved by the Board of Directors and implemented by senior management.

ANNEX 4: Operational Risk

Operational risk is the risk of loss arising from complex operations, inadequate internal controls, processes and information systems, organizational changes, fraud or human errors, or unforeseen catastrophes (including terrorist attacks and natural disasters).

1. Banks should identify all material sources of operational risk, including:

   (a) potential criminal action, including fraud and theft, by external parties and by the bank's own staff or contractors, including misappropriation of customer funds;

   (b) interruption/failure of IT or communication systems;

   (c) disruption due to weather events (flood, storm etc.), other natural disasters, failures in physical security or protection of the bank's assets;

   (d) breaches in IT and data security such as cyberattacks;

   (e) loss of customers' or other sensitive data or other failures to protect customer privacy;

   (f) failures of process, for example in payments and settlements, disbursement of loans, repayment of deposits, accounting and financial control;

   (g) human error, for example due to inadequate recruitment, training or management of human resources, including high staff turnover; and

(h) failures by providers of outsourced services, correspondent banks etc.

2. Banks should <u>measure</u> all their material operational risks, adopting appropriate measurement techniques such as:

(a) use of data on loss events, both internal loss data and data on external operational risk events, where available, to assess the bank's vulnerability to similar losses;

(b) risk and performance indicators (key risk indicators) such as the level of staff turnover, transaction volumes and number of failed trades (transactions that do not settle), downtime of key IT systems etc.;

(c) testing of processes such as payments or of controls to assess loss potential;

(d) risk control self–assessments (questionnaires completed by business units setting out their vulnerabilities to failure of controls);

(e) stress tests and simulations, for example to assess the impact of IT failures, natural disasters etc. (see separate Guideline to be issued by the CBM).

3. Banks should <u>monitor</u> operational risks. They should:

(a) collect data on loss events, assess trends, including vulnerabilities to events captured in external loss data, and make reports to senior management and the Board;

(b) ensure that management information systems (MIS) capture information on operational risk across all the bank's activities that is accurate and regularly updated.

4. Banks should <u>control</u> operational risks. They should:

(a) develop a Board–approved statement of their tolerance for operational risk losses;

(b) establish policies and processes for mitigating operational risk, for example by:

(i) strengthening of controls in areas identified as vulnerable to operational loss;

(ii) increasing physical and IT security;

(iii) using insurance to mitigate losses when they occur;

(iv) taking back services provided by outsourcing;

(v) enhancing recruitment policies and procedures such as staff screening;

(vi) increasing staff numbers and skills, including by training;

(c) establish within the risk management function reporting to the chief risk management officer an operational risk unit or person responsible for bank–wide operational risk;

(d) establish processes for ensuring that new products and activities are evaluated for their impact on the bank's operational risk and the risk falls within its risk tolerance;

(e) undertake internal audit work on the effectiveness of controls over operational risk.

5. Banks should develop a Board–approved business continuity plan as a key control over operational risk. The plan should:

(a) set out the actions to be taken to recover core business operations in case of an interruption, for whatever cause;

(b) include arrangements for switching data processing and other core IT systems and databases to a back–up site or outsourced service provider;

(c) set out responsibilities for activating the plan where necessary; and

(d) be subject to regular testing, involving key service providers as appropriate, with appropriate monitoring of test results and responses to the lessons learned.

6. The bank should have a comprehensive strategy for managing its IT risks, including cyber–resilience and the risks in outsourced IT services. It should:

(a) have a Board–approved framework of controls over IT and data security, including access and password controls etc.;

(b) adopt a comprehensive approach to cyber–resilience, enabling it to anticipate and adapt to threats and withstand, contain and rapidly recover from cyber incidents;

(c) maintain an incident response plan to deal with material cyber–incidents;

(d) appoint a chief information security officer responsible for IT security and resilience.

7. Banks should document their policy on operational risk, covering their tolerance for loss due to operational events, risk measurement methodologies and risk management tools, internal reporting on operational losses, the assessment of new products or activities from the perspective of operational risk, and business continuity plans. Banks' policies should be approved by the Board of Directors and implemented by senior management.

Annex 5: Legal, Regulatory and Reputational Risk

Legal, regulatory and reputational risk is the risk to the bank from exposure to the impact of legal challenge, to changes in the CBM's and other regulation and to the damaging impact of its actions (and those of customers, shareholders etc.) on its reputation, adversely affecting its performance and financial condition.

1. Banks should <u>identify</u> all sources of material legal, regulatory and reputational risk in their business, including risks arising from such sources as:

   (a) inadequate legal documentation (of loans and other contracts) or legal process etc.;

   (b) lack of enforceable title to the bank's assets;

   (c) failure to perfect the bank's interest in collateral, resulting in failure to foreclose;

   (d) limited access to internal legal expertise, external legal advice or legal representation in case of disputes/litigation;

   (e) the impact of legal or regulatory change or failure to implement regulations, including AML/CFT requirements;

   (f) changes in law, regulation or the legal system (including Court procedures), adversely affecting the bank's customers;

   (g) action by the bank that exposes it to criticism resulting in loss or reputational damage, such as failure to treat customers fairly, the use of opaque structures or transactions and unsuitable investments by the bank;

(h) association with customers, directors and staff, shareholders and other stakeholders of the bank who are subject to adverse publicity, affecting the reputation of the bank.

2. Banks should measure their material legal, regulatory and reputational risks, adopting appropriate measurement techniques. Although these risks are hard to measure quantitatively, banks should seek to evaluate their scale and potential significance by reference to the value of transactions exposing them to risk, losses incurred (including by other banks) as a result of these risks and other measures. They should be able to describe qualitatively the nature and scale of these risks, taking into account their business model, the nature of their customers etc.

3. Banks should monitor their material legal, regulatory and reputational risks. They should:

(a) collect data on losses or reputational damage that has been incurred and monitor changes to the bank's business model and customer base, significant transactions and developments affecting major customers etc.;

(b) ensure that management information systems (MIS) capture information on the bank's risks that is accurate, regularly updated and covers all the banks' activities.

(c) make regular reports on legal, regulatory and reputational risk to senior management, the Board Risk Management Committee or Audit Committee and to the Board.

4. Banks should <u>control</u> all material legal, regulatory and reputational risk. They should:

(a) establish and monitor compliance with a Board–approved tolerance for legal, regulatory and reputational risk, covering all types and sources of risk;

(b) ensure that there is adequate legal review of significant contract documentation, including for loans and other credit facilities, foreign exchange business and for collateral arrangements;

(c) establish a compliance function with responsibilities including:

(i) to advise business units, other control functions and the Risk Management Committee of the implications of relevant laws and regulations;

(ii) to review all significant new laws, regulations and other regulatory initiatives to identify actions that the bank should take to ensure compliance;

(iii) to review and approve new products and services to reduce the risk that the new activity may not be compliant with all applicable laws and regulations;

(iv) to monitor and report on the bank's compliance with laws, regulations and relevant internal policies;

(d) assess new customers and periodically review existing customers to identify potential reputational risks;

(e) establish policies and procedures on:

(i) the fair treatment of the bank's customers (retail customers, in particular) to mitigate risk of legal and reputational damage due to the bank's misconduct; and

(ii) the bank's investments, including its establishment of subsidiaries, to mitigate the risk of unsuitable investments leading to legal or reputational risk;

(f) establish levels of authority for approving products, transactions, customers and investments that give rise to legal, regulatory and reputational risks;

(g) establish within the risk management function reporting to the chief risk management officer a legal, regulatory and reputational risk unit or person responsible for bank–wide risks; the responsibilities of the risk management and compliance functions should be defined to promote cooperation on the management of legal, regulatory and reputational risks, while preserving the independence of each function;

(h) undertake regular internal audit work on the effectiveness of controls over legal, regulatory and reputational risk, including the effectiveness of the compliance function.

5. Banks should <u>document</u> their policies and procedures on legal, regulatory and reputational risk, covering their risk tolerance, their procedures for identification, measurement, monitoring and control of legal, regulatory and reputational risk. Banks' policies should be approved by the Board of Directors and implemented by senior management.

Annex 6: Strategic risk

Strategic risk is the risk that the bank fails to maintain an appropriate strategy that responds to market and wider environmental challenges, adversely affecting its performance and financial condition.

1. Banks should identify all sources of material risk to successful implementation of their strategy, such as:

   (a) adverse developments in the economy or in financial variables such as interest and exchange rates;

   (b) increased competition, including from non–bank financial institutions and entry of banks from outside Myanmar;

   (c) changes in laws, regulations and applicable accounting standards, in Myanmar or internationally;

   (d) inadequate staff numbers or skills (including IT, project management, accounting and other specialist skills);

   (e) lack of, or limitations on other resources, including financial resources, IT capacity, access to audit or consultancy services;

   (f) unexpected changes in customer requirements for banking products and services;

   (g) unexpected changes in delivery channels, for example mobile banking;

   (h) failure to identify risks to the bank's strategy and to respond appropriately;

(i) failure to communicate the strategy effectively, within the bank and to stakeholders;

(j) inadequacies in the process for developing the bank's strategy or weaknesses in the bank's organization or governance;

(k) lack of adequate Board or senior management attention to strategic issues, for example because of the need to address legacy issues such as non–performing loans.

2. Banks should <u>monitor</u> and <u>control</u> key strategic risks. They should establish Board–approved processes for:

(a) developing and adopting the bank's strategy that:

(i) define responsibilities, including those of senior management and the Board;

(ii) ensure the involvement of business units, control functions, operations and administrative functions of the bank and other stakeholders, as appropriate;

(iii) ensure that the strategy is based on realistic assumptions about macroeconomic conditions, regulation, competition, access to capital and funding, staffing, IT resources etc.; and is consistent with the bank's risk appetite; and

(iv) ensure that the agreed strategy is reflected in business unit plans, financial projections (income and expenditure budgets) and the capital management plan; and is communicated effectively to stakeholders;

(b) monitoring implementation of the strategy and associated business plans, including the validity of underlying assumptions; and

(c) reviewing the strategy on a regular basis, including:

(i) regular testing of key assumptions such as those related to macroeconomic and financial conditions, customer needs and likely future demand for banking services;

(ii) evaluating the reasons for divergence between outcomes and plans, including financial performance;

(iii) identifying where the strategy needs to be changed and the timeframe for implementing any changes;

(iv) identifying and planning for any associated changes in the resources required to implement the strategy or in the bank's organization and governance; and

(v) reviewing and updating the bank's assessment of risks to the successful implementation of the strategy and actions to be taken to mitigate those risks.

3. The bank should consider whether to maintain contingency plans so that it can take appropriate action in case its strategic objectives are at risk. These plans could include raising additional capital, recruiting specific expertise or engaging external advisors as well as discontinuing certain activities. Its contingency plans should be consistent with its capital management and business continuity plans.

4. The bank should undertake regular internal audit reviews of the effectiveness of its controls over strategic risk, including its processes for developing, implementing, monitoring, reviewing and updating its strategy and for assessing and mitigating the risks to successful implementation of the strategy.

Annex 7: Group and Related Parties Risk

Group and related parties risk is the risk to a bank resulting from its membership of a group of companies or its exposure to loss or reputational damage as a result of transactions or association with related parties.

1. Banks should identify all sources of material group and related parties risk, such as:

   (a) loans and other credit facilities made available to other parts of the bank's group or to other related parties as defined in the FIL Section 64 and the CBM's Related Parties Directive (No. 11/2019);

   (b) guarantees or collateral given, performance bonds and other commitments;

   (c) exposures to loss due to impairment of investments in subsidiaries or contagion from financial weakness elsewhere in the bank's group;

   (d) exposures to its staff under arrangements for staff to receive loans;

   (e) exposure to reputational damage due to adverse developments affecting other parts of the bank's group or its related parties;

   (f) exposures related to rendering or receiving of services from other entities within the bank's group or related parties, in particular where the bank is dependent on significant services provided by a group company or related party;

(g) risks relating to transfers, purchases and sales of goods, property and other assets with members of the same group or other related parties; and

(h) risks relating to any other transactions with group and related parties, such as settlement of the liabilities of a related party.

2. Banks should <u>measure</u> all their material group and related parties risks. They should:

(a) establish processes to identify all the other members of the group of which they are a part and all their other related parties; banks should seek access to:

(i) details of the structure and organization of its group, its major shareholders, and senior management;

(ii) financial information on the group and significant companies, including the group’s consolidated annual financial statements and audit report as well as the audited financial statements of other members of the group; and

(iii) the group’s governance arrangements, risk management and internal control procedures;

(b) assess the risks to the bank of membership of the group and its relationships with other related parties; the assessment should be quantitative, where possible (including analysis of the group’s financial condition using debt to equity ratios, profitability ratios etc.); and qualitative where necessary, drawing on discussion with the management of the group.

3. Banks should <u>monitor</u> and <u>control</u> their material group risks. They should:

(a) regularly review exposures to group companies and other related parties and make reports to senior management, the Board Risk Management Committee, where applicable, and Board of Directors on their exposures;

(b) establish controls to ensure that exposures to members of the bank's group and its related parties are identified, including procedures to assess whether new customers are related to the bank;

(c) establish controls to ensure that credit facilities and other transactions undertaken with group members and other related parties are undertaken on market terms and conditions as required by the CBM's Related Parties Directive (No. 11/2019);

(d) develop policies and procedures to mitigate its risks by:

(i) establishing limits on exposures to other members of the bank's group and related parties, in compliance with the FIL and CBM's requirements, and including limits on its use of services provided by the group;

(ii) requiring collateral or guarantees or other mitigants of risk in relation to group and related party exposures;

(iii) ensuring that no assets of other group companies (or those of shareholders) are identified in the bank's books and records as the property of the bank; and

(iv) cooperating with the management of the group to promote effective risk management at the group level;

(e) establish processes and controls to ensure that:

(i) where the FIL requires that transactions be approved by the Board of Directors before they may be entered into by the bank, such approval is sought and obtained and the approval recorded;

(ii) where the FIL requires that transactions be secured by collateral before they may be entered into by the bank, the bank has processes and controls to ensure that collateral is provided, that it is of adequate quality, subject to appropriate valuation procedures and has been taken under appropriate legal agreements; and

(iii) the Board of Directors is notified of all related party exposures and transactions and that write–offs of all related party exposures are subject to approval of the Board;

(f) establish a policy for transactions with employees, including staff loans and controls to ensure that any lending is compliant with the terms of the policy.

4. The bank should undertake regular internal audit reviews of the effectiveness of its controls over group and related parties risk.

5. Banks should <u>document</u> their policies and procedures on group and related parties risk, covering the exposures they are prepared to accept and their procedures for identification, measurement, monitoring and control of the risks. Banks' policies should be approved by the Board of Directors and implemented by senior management.