EC No. 38 / DoS – 04 / 2023-2024 14 March 2024

Ref. No. NB. HO. DoS. Pol. / 4291 / J-1 / 2023-2024

The Chairman, Regional Rural Banks
The Managing Director, All State Cooperative Banks
The Managing Director/ Chief Executive Officer,
All District Central Cooperative Banks

Madam/Dear Sir,

Guidance Note on Operational Risk Management (ORM)

Financial institutions are operating in an ever-evolving business environment where complexities and uncertainties are inevitable and the need for Operational Risk Management (ORM) stands out as a paramount imperative. ORM is a strategic approach that organisations must embrace to fortify themselves against potential disruptions, ensuring financial stability, regulatory compliance, and sustained trust among stakeholders.

2. NABARD had issued detailed guidance note on ORM vide Circular No. 31/DoS-06/2010 dated 05 February 2010 for Regional Rural Banks. As a supervisor, NABARD consistently adjusts its supervisory methods to align with the evolving rural financial landscape. This includes regular reviews, updates to guidelines, scheduled inspections, and rigorous monitoring of banks' compliance submissions. Reflecting the shift towards a risk-based supervisory approach, the Enhanced CAMELSC-based framework was implemented for a specific set of Supervised Entities (SEs) starting April 1, 2023. Integration of this framework into the supervision of remaining SEs will occur gradually. A key feature of the Enhanced CAMELSC framework is its ability to offer a forward-looking risk intelligence perspective on SEs, facilitating early intervention by supervisors.

3. To bridge the supervisory gaps between E-CAMELSC and existing CAMELSC, and also to guide our SEs to secure themselves from the emerging operational risks; the guidance note on ORM has been updated to provide clear insights, practical methodologies and actionable steps for identifying, assessing, monitoring, and mitigating operational risks. This revision aims to help SEs understand how to incorporate operational risk considerations and establish a resilient internal check and control system, protecting them from both internal and external disruptions.

4. This guidance note provides an outline of a set of sound principles for effective management and supervision of operational risk to be practiced by Supervised Entities (SEs). We shall be glad if you will place a copy of this circular before the next meeting of the Board of Directors of your bank so as to take a suitable decision on implementation of the guidelines in your bank. SEs are advised to put in place appropriate mechanism to implement the Operational Risk Management policies and the relevant frameworks as mentioned in the guidance note by **31 March 2024.**

5. Please acknowledge the receipt of this circular to our Regional Office in your State/ UT.

Yours faithfully

Sd/-
(Sudhir Kumar Roy)
Chief General Manager

Encl: Guidance note

Main Document

Document title	Guidance Note on Operational Risk Management
Drafted by	Department of Supervision
Date of approval	20 December 2023
Document classification	External
Document no. / Version no.	2.0

Version history

Version no.	FY	Changes / Comments	Changed by
1.0	2009-10	-	Department of Supervision
2.0	2023-24	Overall review	Department of Supervision

Version Approval

Version no.	Date of approval	Changes / Comments	Approved by
1.0	05 February 2010	-	Board of Supervision
2.0	20 December 2023	Overall review	Board of Supervision

References

Sr. no.	Reference	Reference no
1	Guidance Note on Operational Risk management	Circular no. 31 / DOS-06/ 2010, Ref. no. NB.DoS.HO.POL./4773/J-1/2009-10

Guidance Note on Operational Risk Management

Table of Contents

Executive Summary

The rise in significant operational loss events globally has led banks and regulators to acknowledge Operational Risk Management (ORM) as a vital part of overall risk management. While managing specific operational risks like fraud prevention and maintaining internal control integrity has long been crucial for banks, what is relatively new is the recognition of ORM as a comprehensive practice comparable to managing credit and market risk. The term 'management' of operational risk includes the processes of identifying, assessing, measuring, monitoring, and controlling/ mitigating such risks.

1.2 The guidance note is structured into seven chapters. It defines operational risk and its likely manifestation in **Chapter 1**. In order to create an enabling organisational culture and placing high priority on effective ORM and implementation of risk management processes, **Chapter 2** gives a typical outline of the organisational set-up in the banks, together with the responsibilities of the Board and senior management in the banks. **Chapter 3** deals with the policy requirements and strategic approach to ORM. The policies and procedures should outline all aspects of the bank's ORM framework. **Chapter 4** deals with issues of identification and assessment of operational risk**. Chapter 5** deals with monitoring of operational risk. This chapter has put in one place the business lines that a bank needs to identify and the principles underlying mapping of these business lines. Details of effective control/mitigation of operational risk are dealt in **Chapter 6.** Internal audit and its scope for an independent evaluation of the ORM function are dealt under **Chapter 7.** Although the guidance note is an outline of sound principles for effective management and supervision of operational risk by banks, this guidance note does not deal with capital allocation methodology for operational risk as capital allocation for operational risk based on basic indicator approach has not been made applicable to RRBs and StCBs / DCCBs.

1.3 The specific approach to ORM adopted by banks will vary based on a multitude of factors. Despite these differences, certain key components are universally essential for an effective ORM framework. These include clear strategies and oversight by Board of Directors and senior management, fostering a robust ORM culture, implementing effective internal controls and reporting mechanisms, and establishing contingency planning. In pursuit of a comprehensive ORM strategy, initiatives required to be taken by banks in this regard will include the following:

- Board of Directors bears primary responsibility for ensuring the effective management of operational risks in banks. They are tasked with overseeing that senior management establishes and maintains a robust system of internal controls.
- ORM should be identified and introduced as an independent risk management function across the entire bank.
- The senior management must have clearly defined responsibilities for implementing ORM as approved by the Board of Directors.
- Board of Directors and senior management are responsible for creating awareness of operational risks and establishing a culture within the bank that

emphasizes and demonstrates to all the levels of personnel the importance of operational risk.

- The direction for effective ORM should be embedded in the policies and procedures that clearly describe the key elements for identifying, assessing, monitoring and controlling / mitigating operational risk.
- The internal audit function plays a crucial role in assisting the senior management and the Board by independently reviewing application and effectiveness of ORM procedures and practices approved by the Board/ senior management.
- Banks have not been required to calculate operational risk capital charge for the present.

Chapter 1

Introduction

1.1 Financial institutions are in the business of risk management and hence are incentivised to develop sophisticated risk management systems. The basic components of a risk management system are identifying the risks the entity is exposed to, assessing their magnitude, monitoring them, controlling or mitigating them using a variety of procedures.

1.2 Financial institutions, driven by the core nature of risk management in their operations, are motivated to cultivate advanced risk management systems. A comprehensive risk management framework involves identifying the array of risks to which the institution is exposed, assessing their magnitude, vigilant monitoring, and implementing control or mitigation measures through various procedures. This proactive approach not only enhances the institution's resilience but also underscores its commitment to navigating the intricate landscape of risks inherent in the financial sector.

1.3 The convergence of financial services deregulation coupled with increasing adoption of financial technology is imparting greater complexity to the activities and profiles of banks. As banking practices continue to evolve, it becomes evident that risks beyond traditional credit and market risks can be significant. Emerging risks faced by banks encompass a spectrum of challenges due to highly automated technology, emergence of E-Commerce, increased outsourcing of services, mergers and consolidations, etc.

Definition

1.4 Operational risk has been defined by the Basel Committee on Banking Supervision as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk. This definition is based on the underlying causes of operational risk. It seeks to identify why a loss happened and at the broadest level includes the breakdown by four causes: people, processes, systems and external factors.

- People: Risk related to placement, competency, work environment, motivation, turnover/ rotation.
- Process:
    a) Transaction Risk - Transaction guidelines, errors in execution of transaction, product complexity, competitive disadvantage, documentation /contract risk.
    b) Operational Control Risk - violation of controls, operational disruptions exceeding of limits, money laundering, fraud, etc.
- Systems Risk:
    a) Technology Risk - system failure, system security, programming error, communications failure, etc.
    b) Management Information Systems (MIS) Risk.

- External Factors:
    a) Legal and Regulatory Risk - includes but not limited to exposure to fines, penalties or punitive damages resulting from supervisory actions as well as private settlements. It can also be defined as failing to comply with laws and regulations (e.g. environment, data protection, labour, taxation, money laundering) to protect fully banks' legal rights and to observe contractual commitments.
    b) Event Risk – An example would be Operating Environment Risk (external factors risk) wherein unanticipated changes in external environment, other than macro-economic factors, take place.

Likely forms of manifestation of operational risk

1.5 A clear appreciation and understanding by banks of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important to consider the full range of material operational risks facing the bank and capture all significant causes of severe operational losses. Operational risk is pervasive, complex and dynamic. Unlike market and credit risk, which tend to be in specific areas of business, operational risk is inherent in all business processes. Operational risk may manifest in a variety of ways in the banks.

1.6 Basel Committee has identified the following types of operational risk events as having the potential to result in substantial losses:

- **Internal fraud:** For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
- **External fraud:** For example, robbery, forgery, check kiting, and damage from computer hacking.
- **Employment practices and workplace safety:** For example, workers compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims, and general liability.
- **Clients, products and business practices:** For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorised products.
- **Damage to physical assets:** For example, terrorism, vandalism, earthquakes, fires and floods.
- **Business disruption and system failures:** For example, hardware and software failures, telecommunication problems, and utility outages.
- **Execution, delivery and process management:** For example, data entry errors, collateral management failures, incomplete legal documentation, and unauthorised access given to client accounts, non-client counterparty mis-performance, and vendor disputes.

Chapter 2

Organisational set-up and Key Responsibilities for ORM

Relevance of Operational Risk Function

2.1 The growing prevalence of significant operational loss events worldwide has compelled both banks and supervisors/regulators to increasingly recognize Operational Risk Management (ORM) as an integral and indispensable component of overall risk management practices. The management of specific operational risks, such as fraud prevention, maintaining internal control integrity, and reducing errors in transaction processing, is not a recent development and has long been crucial for banks. What is relatively new is the perception of ORM as a comprehensive practice comparable to the management of credit and market risk. The term 'management' of operational risk encompasses the 'identification, assessment, and/or measurement, monitoring, and control/mitigation' of this risk.

2.2 Operational risk differs from other banking risks in that it is typically not directly taken in return for an expected reward but is implicit in the ordinary course of corporate activity and has the potential to affect the risk management process. However, it is recognized that in some business lines with minimal credit or market risks, the decision to incur operational risk, or compete based on the perceived ability to manage and effectively price this risk, is an integral part of a bank's risk/reward calculus. At the same time, failure to properly manage operational risk can result in a misstatement of an institution's risk profile and expose the institution to significant losses.

Organisational Set up and Culture

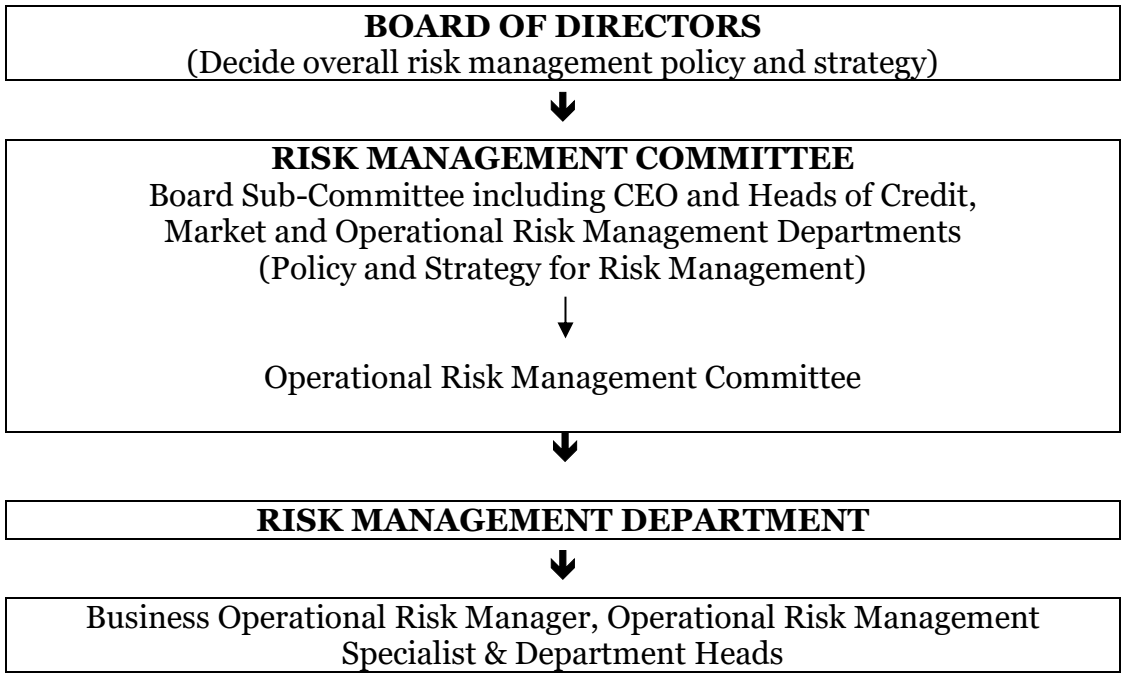
2.3 Operational risk is intrinsic to a bank and should be an important component of its risk management systems. Board and senior management should create an enabling organizational culture placing high priority on effective ORM and adherence to sound operating procedures. Successful implementation of risk management process has to emanate from the top management with the demonstration of strong commitment to integrate the same into the basic operations and strategic decision making processes. Therefore, Board and senior management should promote an organisational culture for management of operational risk.

2.4 It is recognised that the approach for ORM that may be chosen by an individual bank will depend on a range of factors, including size and sophistication, nature and complexity of its activities. However, despite these differences, clear strategies and oversight by the Board of Directors and senior management; a strong operational risk culture, i.e., the combined set of individual and corporate values, attitudes, competencies and behavior that determine a bank's commitment to and style of ORM; internal control culture (including clear lines of responsibility and segregation of duties); effective internal reporting; and contingency planning are all crucial elements of an effective ORM framework.

2.5 Ideally, the banks, looking to their size and volume of business operations, need not go in for a very detailed organizational set-up for ORM as in the case of Commercial Banks but should include the following:

- Board of Directors
- Risk Management Committee of the Board
- Operational Risk Management Committee/Department
- Support Group for ORM

2.6 A typical organizational chart for supporting ORM function in banks could be as given below:



2.7 It has to be ensured that each type of major risk viz. credit risk, market risk and operational risk, is managed as an independent function. However, banks may not have corresponding risk management committees, which are assigned the specific responsibilities in view of their limited size and volume of operations. Banks may structure the risk management department(s) as appropriate without compromising on the above principles, based on their risk perception, size and volume of operations.

Responsibilities of Board:

2.8 Board of Directors of a bank is primarily responsible for ensuring effective management of operational risks. Board would include Committee of the Board to which the Board may delegate specific ORM responsibilities:

- Board of Directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve an appropriate ORM framework for the bank and review it periodically.
- Board of Directors should provide senior management with clear guidance and direction.
- ORM Framework should be based on appropriate definition of operational risk which clearly articulates what constitutes operational risk in the bank and covers the bank's appetite and tolerance for operational risk. The framework

should also articulate the key processes the bank needs to have in place to manage operational risk.

- Board of Directors should be responsible for establishing a management structure capable of implementing the bank's ORM framework. Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the Board establishes clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflicts of interest.
- Board shall review the framework regularly to ensure that the bank is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems. This review process should also aim to assess industry best practice in ORM appropriate for the bank's activities, systems and processes. If necessary, the Board should ensure that the ORM framework is revised in light of this analysis, so that material operational risks are captured within.
- Board should ensure that the bank has in place adequate internal audit coverage to satisfy itself that policies and procedures have been implemented effectively. The ORM framework should be subjected to an effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff **not directly involved in the ORM process**.
- Though, in smaller banks, the internal audit function may be responsible for developing the ORM programme, responsibility for day-to-day operational risk management should be transferred elsewhere.
- Board should receive regular and focused training to understand and execute its ORM responsibilities, such as ethics, fraud management, business continuity, succession planning, etc.

Responsibilities of Senior Management

2.9 Senior management should have responsibility for implementing the ORM framework approved by the Board. The framework should be consistently implemented throughout the whole bank, and all levels of staff should understand their responsibilities with respect to ORM. The additional responsibilities that devolve on the senior management include the following:

- To translate ORM framework established by the bank's Board into specific policies, processes and procedures that can be implemented and verified within the different business units. Senior management should be responsible for implementation of the strategy, policies and processes pertaining to ORM.
- To clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability and ensure that necessary resources are available to manage operational risk effectively.
- To assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy.
- To ensure bank's activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources, and that staff responsible for monitoring and enforcing compliance with the institution's risk policy have authority independent from the units they oversee.

- To ensure that the bank's ORM policy has been clearly communicated to staff at all levels.
- To ensure that staff responsible for managing operational risk communicate effectively with staff responsible for managing credit, market, and other risks as well as with those in the bank who are responsible for the procurement of external services, such as, insurance purchasing and outsourcing agreements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.
- To give particular attention to the quality of documentation controls and transaction-handling practices. Policies, processes and procedures related to high transaction volumes, in particular, should be well documented and disseminated to all relevant personnel.
- To ensure that the bank's HR policies are consistent with its appetite for risk and are not aligned to rewarding staff who deviate from policies.

2.10 The broad indicative role of each organizational arm of the risk management structure both at the Head Office level and at the functional level is indicated in brief in **Annexure 1.** These can be customized to the actual requirements of each bank depending upon the size, risk profile, risk appetite and level of sophistication.

Chapter 3

Policy Requirements and Strategic Approach

3.1 The ORM framework provides the strategic direction and ensures that an effective operational risk management and measurement process is adopted throughout the bank. Each bank's operational risk profile is unique and requires a tailor-made risk management approach appropriate for the scale and materiality of the risk present, and the size of the institution. There is no single framework that would suit every bank. In fact, many ORM techniques continue to evolve rapidly to keep pace with new technologies, business models and applications. Operation risk is more a risk management than measurement issue. **The key elements in the ORM process** include –

- Appropriate policies and procedures.
- Efforts to identify and measure operational risk.
- Effective monitoring and reporting.
- A sound system of internal controls.
- Appropriate testing and verification of the Operational Risk Framework.

Policy Requirement

3.2 Each bank must have policies and procedures that clearly describe the major elements of the ORM framework including identifying, assessing, monitoring and controlling / mitigating operational risk.

ORM policies, processes, and procedures should be documented and communicated to appropriate staff. The policies and procedures should outline all aspects of the bank's ORM framework, including: -

- The roles and responsibilities of the independent bank-wide ORM function and line of business management.
- A definition for operational risk, including the loss event types that will be monitored.
- The capture and use of internal and external operational risk loss data including data potential events.
- The development and incorporation of business environment and internal control factor assessments into the operational risk framework.
- A description of the internally derived analytical framework that quantifies the operational risk exposure of the institution.
- A discussion of qualitative factors and risk mitigants and how they are incorporated into the operational risk framework.
- A discussion of the testing and verification processes and procedures.
- A discussion of other factors that affect the measurement of operational risk.
- Provisions for the review and approval of significant policy and procedural exceptions.
- Operational risk limits, breach of limits and reporting levels.
- Regular reporting of critical risk issues facing the banks and its control/mitigations to senior management and Board.

- Top-level reviews of the bank's progress towards the stated objectives.
- Checking for compliance with management controls.
- Provisions for review, treatment and resolution of non-complied issues.
- A system of documented approvals and authorisations to ensure accountability at an appropriate level of management.
- Define the risk tolerance level for the bank, break it down to appropriate limits, and prescribe reporting levels and breach of limits.
- Indicate the process to be adopted for immediate corrective action.

3.3 Given the vast advantages associated with effective ORM, it is imperative that the strategic approach of the risk management function should be oriented towards:

- Minimising and eventually eliminating losses and customer dissatisfaction due to failures in processes.
- Focus on flaws in products and their design that can expose the institution to losses due to fraud, etc.
- Align business structures and incentive systems to minimize conflicts between employees and the institution.
- Analyze the impact of failures in technology / systems and develop mitigants to minimize the impact.
- Develop plans for external shocks that can adversely impact the continuity in the bank's operations.

Banks can decide upon the mitigants for minimizing operational risks rationally, by looking at the costs of putting in mitigants as against the benefit of reducing the operational losses.

Key Elements of the ORM Framework

3.4 A robust ORM framework is indispensable for a bank to achieve optimal risk management. This document provides an overarching view of the key components within the ORM framework and the details of the same are at a broader level viz.,

- **Risk and Control Self-Assessment (RCSA) Framework:** Identification and assessment of 'inherent' risks in process; identification of specific controls, assessment and rating of the controls, assessment of 'residual' risk, generation of health index for the RCSA entity culminating in reporting of RCSA results and evolving appropriate action plan to improve the health index. For more details, refer to **Annexure 3.**

- **Key Risk Indicators (KRI) Framework** details about early warning signals, which enable the management to monitor and mitigate operational risks that are exceeding acceptable levels. These are statistics and/or metrics, which can provide insight into a bank's operational risk profile and its changes. For more details, refer to **Annexure 4.**

- **New Product Approval Framework (NPAF)** aims to bring in structured approach to launch new products/ processes or modifications in the existing products with a view to meet standards like adherence to regulatory

requirements, obtaining approval of the competent departments and to put in place risk mitigation measures. For more details, refer to **Annexure 5.**

- **Incident and Loss Data Management (ILDM)** is a tool that aims for an effective, timely and consistent reporting, documentation, analysis and monitoring of the operational losses and near miss events. The tool may facilitate taking preventive measures for minimizing the future recurrence of similar loss. For more details, refer to **Annexure 6.**

Chapter 4

Identification and Assessment of Operational Risk

4.1 Banks are mostly relying upon internal control mechanisms within business lines, supplemented by the audit function, to manage operational risk. While these remain important, there is need to adopt specific structures and processes aimed at managing operational risk. Several recent cases demonstrate that inadequate internal controls can lead to significant losses for banks. The types of control breakdowns may be grouped into five categories:

i. *Lack of Control Culture* - Management's inattention and laxity in control culture, insufficient guidance and lack of clear management accountability.
ii. *Inadequate recognition and assessment of the risk of certain banking activities*, whether on-or-off-balance sheet. Failure to recognise and assess the risks of new products and activities or update the risk assessment when significant changes occur in business conditions or environment.
iii. *Absence/failure of key control structures and activities,* such as segregation of duties, approvals, verifications, reconciliations and reviews of operating performance.
iv. *Inadequate communication of information between levels of management within the bank* – upward, downward or cross-functional.
v. *Inadequate / ineffective audit/monitoring programs*.

4.2 Managing operational risk is emerging as an important feature of sound risk management practice in the wake of phenomenal increase in volume of transactions, high degree of structural changes and complex technological support systems. Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. Some of the guiding principles for the banks to manage operational risks are identification, assessment, monitoring and control of these risks which are dealt in detail below:

Identification of operational risk

4.3 Risk identification and assessment are fundamental characteristics of an effective ORM system. Effective risk identification considers both internal factors (e.g., the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes, employee turnover, etc.) and external factors (e.g., changes in the broader environment & the industry, advances in technology, etc). Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively. Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Such identification should also be attributed to certain key risk factors and triggers. Banks should also ensure that before new products, activities, processes and systems are introduced/undertaken, the operational risk inherent in them is identified clearly and subjected to adequate assessment procedures.

4.4 The first step towards identifying risk events is to list out all the activities that are susceptible to operational risk. Usually this mapping of business lines is carried out at several ' levels'. For more details, refer to **Table 1 of Annexure 2.**

- Level 1 - lists the main business groups viz., retail banking, commercial banking, agency services, payment and settlement, asset management, and retail brokerage.
- Level 2 - lists out the product teams in these business groups, e.g. transaction banking, general banking, cash management, securities markets, etc.
- Level 3 - lists out the product offered within these business groups by each product team, e.g. letter of credit, bank guarantee, etc., which can be analysed.
- If required, a fourth level can be added.

4.5 After the products are listed, the various operational risk events associated with these products are recorded based on the risk events referred to in **Annexure 2, Table 2**. An operational risk event is an incident/experience that has caused or has the potential to cause material loss to the bank either directly or indirectly with other incidents. Risk events are associated with the people, process and technology involved with the product. They can be recognized by:

- Experience - The event has occurred in the past.
- Judgment - Business logic suggests that the bank is exposed to a risk event.
- Intuition - Events where appropriate measures saved the institution in the nick of time.
- Linked Events - This event resulted in a loss resulting from other risk type (credit, market etc.).
- Regulatory requirement – Regulator requires recognition of specified events.

These risk events can be catalogued under the last tier for each of the "Level 3" products at a minimum or as per the decisions of the senior management.

Assessment of Operational Risk

4.6 In addition to identifying the risk events, banks should also assess their vulnerability to them. Effective risk assessment allows a bank to better understand its risk profile and most effectively target risk management resources. Amongst the possible tools that may be used by banks for assessing operational risk are:

- **Risk and Control Self-Assessment**: A bank assesses its operations and activities against a menu of potential operational risk vulnerabilities as listed in the RCSA framework. RCSA, typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered). This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them. Banks can adopt their own method of scorecards based on their risk perception and business practices.

Indicative details of RCSA:

Process	Sub-Process	Inherent risk description	Probability rating	Impact rating	Risk type	Control description	Control type	Control owner	Control test steps	Test results	Residual risk rating

- **Risk Mapping**: In this process, various business units, organisational functions or process flows are mapped by risk type (regulatory risk, financial risk, fraud risk, external risk, etc.). This exercise can reveal areas of weakness and help prioritise subsequent management action.

- **Key Risk Indicators**: Key risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators should be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

- **Audit Findings:** Internal Audit is a third line of defense which is independent of management control and reports directly to the Audit Committee of the Board. An effective internal audit reflects the issues and gaps in the processes which are missed by the first line (functional department/unit) and second line (operation risk department) of business.

- **Internal Loss Data Collection and Analysis:** Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic. Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure.

    a. A bank must be able to map its historical internal loss data into the relevant Level-1 supervisory categories defined in **Annexure 2 (Table 1 & 2)** and to provide these data to supervisors upon request to assist in supervisory validation. The banks must have a clear cut documented objective criteria for allocating losses to the specified business lines and event types. However, it is left to the bank to decide the extent to which it applies these categorisations in its internal operational risk measurement system.

    b. Aside from information on gross loss amounts, a bank should collect information about the date of the event, any recoveries of gross loss amounts, as well as some descriptive information about the drivers or causes of the loss event. The level of detail of any descriptive information should be commensurate with the size of the gross loss amount.

    c. A bank may also develop specific criteria for assigning loss data arising from an event in a centralised function (e.g. an information technology

department) or an activity that spans more than one business line, as well as from related events over time.

d. A bank's internal loss data must be comprehensive and should capture all material activities and exposures from all appropriate sub-systems and geographic locations. A bank must be able to justify that any excluded activities or exposures, both individually and in combination, would not have a material impact on the overall risk estimates.

- **External Data Collection and Analysis:** External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at outside organisations other than the bank. The bank may use external data collection and analysis for the identification of operational risk when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses. External loss data can be compared with internal loss data or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures.

- **Comparative Analysis:** Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank determine whether self-assessment processes are functioning effectively. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank's exposure to potential risk events.

Measurement

4.7 A key component of risk management is measuring the size and scope of the bank's risk exposures. Banks may develop risk assessment techniques that are appropriate to the size and complexities of their portfolio, their resources and data availability. A good assessment model must cover certain standard features. An example is the "matrix" approach in which losses are categorized according to the type of event and the business line in which the event occurred. Banks may quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. In this way, a bank may identify events which have the most impact across the entire bank and which business practices are most susceptible to operational risk. Once potential loss events and actual losses are defined, a bank can analyze and perhaps even model their occurrence. Doing so requires constructing databases for monitoring such losses and creating risk indicators that summarize these data. Examples of such indicators are the number of failed transactions over a period of time and the frequency of staff turnover within a division.

4.8 Every risk event in the risk matrix is then classified according to its frequency and severity. By frequency, the reference is to the number/ potential number (proportion)

of error events that the product type / risk type point is exposed to. By severity, the reference is to the loss amount/ potential loss amount that the operational risk event is exposed to when the risk event materializes. The classification can be on any predefined scale (say 1-10, low, medium, high, etc.). All risk events will thus be under one of the four categories, namely, high frequency-high severity, high frequency-low severity, low frequency-high severity, low frequency-low severity in the decreasing order of the risk exposure.

4.9 Potential losses can be categorized broadly as arising from "high frequency, low severity" (HFLS) events, such as minor accounting errors or bank teller mistakes, and "low frequency, high severity" (LFHS) events, such as terrorist attacks or major fraud. Data on losses arising from HFLS events are generally available from a bank's internal auditing systems. Hence, modeling and budgeting these expected future losses due to operational risk potentially could be done very accurately. However, LFHS events are uncommon and thus limit a single bank from having sufficient data for modeling purposes. Although qualitative analysis of operational risk is an important input to a bank's risk management systems, these risks cannot be reduced to pure statistical analysis. Hence, qualitative assessments, such as scenario analysis, will be an integral part of measuring a bank's operational risks. Scenarios should be generated for all material operational risks faced by all the organisational units of the bank and assessment of the scenarios may be undertaken.

4.10 Risk assessment should also identify and evaluate the internal and external factors that could adversely affect the bank's performance, information and compliance by covering all risks faced by the bank and operate at all levels within the bank. Assessment should take account of both historical and potential risk events.

Historical risk events are assessed based on:

- Total number of risk events
- Total financial reversals
- Net financial impact
- Exposure: based on expected increase in volumes
- Total number of customer claims paid out
- IT indices: uptime, etc.
- Office Accounts Status: such as changes in balances, debits lying beyond turnaround time, etc.

The factors for assessing potential risks include:

- Staff related factors such as productivity, expertise, turnover.
- Extent of activity outsourced
- Process clarity, complexity, changes
- IT Indices
- Audit Scores
- Expected changes or spurts in volumes

Detailed measurement methods are given in the framework attached as annexures.

Chapter 5

Monitoring of Operational Risk

5.1 An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

5.2 In addition to monitoring operational loss events, banks should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators, an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately. There should be proper capabilities in the system to identify high risk areas and highlight them to the senior management.

5.3 The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of a bank's activities. The results of these monitoring activities should be included in regular management and Board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) intermediary supervisory authorities may also inform the corporate monitoring unit, which should likewise be reported internally to senior management and the Board, where appropriate.

5.4 Senior management should receive regular reports from appropriate areas, such as, business units, group functions, the ORM unit and internal audit. The operational risk reports should contain internal, financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be fully distributed to appropriate levels of management and to areas of the bank on which areas of concern may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these risk reports and audit reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors, etc.) to assess the usefulness and reliability of internal reports. Reports should be analyzed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

Management Information Systems

5.5 Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be a regular reporting of pertinent information to senior management and the Board of Directors that supports the proactive management of operational risk. In general, the Board of Directors should

receive sufficient higher-level information to enable them to understand the banks' overall operational risk profiles and focus on the material and strategic implications for the business. Towards this end, it would be relevant to identify all activities and all loss events in a bank under well-defined business lines.

Business Line Identification

5.6 Banks have different business mixes and risk profiles. Hence, the most intractable problem banks face in assessing operational risk capital is due to this diversity. The best way to get around this intractable problem in computation is by specifying a range of operational risk multipliers for specified distinct business lines. By specifying business lines, banks will be able to crystallise the assessment processes to the underlying operational risk and the regulatory framework. Thus, by specifying business lines, the line managers will be aware of operational risk in their line of business. Further, confusion and territorial overlap which may be linked to subsets of the overall risk profile of a bank can be avoided.

5.7 For the purpose of operational risk management, the activities of a bank may be mapped into the undernoted business lines. The various products launched by the banks are also to be mapped to the relevant business line. Banks must develop specific policies for mapping a product or an activity to a business line and have the same documented to indicate the criteria. The following are indicative list of business lines. Details and methodologies for mapping of these business lines are furnished in **Annexure 2.**

i. Retail Banking
ii. Commercial Banking
iii. Payment and settlement
iv. Agency services
v. Asset management
vi. Retail brokerage

5.8 The following are the principles to be followed for business line mapping:

- All activities must be mapped into the level - 1 business lines in a mutually exclusive and jointly exhaustive manner.

- Any banking or non-banking activity which cannot be readily mapped into the business line framework, but which represents an ancillary function to an activity included in the framework, must be allocated to the business line it supports. If more than one business line is supported through the ancillary activity, an objective mapping criteria must be used.

- The mapping of activities into business lines for ORM must be consistent with the definitions of business lines used for management of other risk categories, i.e. credit and market risk. Any deviations from this principle must be clearly motivated and documented.

- The mapping process used must be clearly documented. In particular, written business line definitions must be clear and detailed enough to allow third parties to replicate the business line mapping. Documentation must, among other things, clearly motivate any exceptions or overrides and be kept on record.

- Processes must be in place to define the mapping of any new activities or products.

- Senior management is responsible for the mapping policy (which is subject to approval by the Board of Directors).

- The mapping process to business lines must be subject to independent review.

5.9 The following principles might be relevant for determining mapping of activities into appropriate business lines:

- Activities that constitute compound activities may be broken up into their components which might be related to the level 2 activities under the business lines. These components of the complex activity may be assigned to the most suitable business lines, in accordance with their nature and characteristics.

- Activities that refer to more than one business line may be assigned to the most predominant business line. If no predominant business line exist, then it may be mapped to the most suitable business lines, in accordance with their nature and characteristics.

Operational Risk Loss Events

5.10 Banks must meet the following data requirement for internally generating operational risk measures:

- The tracking of individual internal event data is an essential prerequisite to the development and functioning of operational risk measurement system. Internal loss data is crucial for tying a bank's risk estimates to its actual loss experience.

- Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological process and risk management procedures. Therefore, banks must have documented procedures for assessing ongoing relevance of historical loss data, including those situations in which judgment overrides, scaling, or other adjustments may be used, to what extent it may be used and who is authorized to make such decisions.

- Bank's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate subsystems and geographic locations. The banks must be able to justify that any of the activities and exposures excluded would not have a significant impact on the overall risk estimates. Banks may have to appropriately minimise the gross loss threshold for internal loss data collection, as may be fixed by their respective of Board of Directors. The appropriate threshold may vary

somewhat between banks and within a bank across business lines and/or event types. However, particular thresholds may be broadly consistent with those used by the peer banks.

- Measuring operational risk requires both estimating the probability of an operational loss event and the potential size of the loss. Operational risk assessment addresses the frequency of a particular operational risk event occurring and the severity of the effect on business objectives.

- Banks must track individual internal actual loss data (i.e., where losses have actually materialised, potential loss, near misses, attempted frauds, etc.) and map the same into the relevant level 1 category defined in **Annexure 2**. Banks must endeavor to map the actual loss events to level 2 as well.

- Operational risk loss would be the financial impact associated with the operational event that is recorded in the financial statement and would include for example, (a) loss incurred, and (b) expenditure incurred to resume normal functioning, but would not include opportunity costs and foregone revenue, etc. However, the banks must also track the potential loss (i.e. extent to which further loss may be incurred due to the same operational risk event), near misses, attempted frauds, etc., where no loss has actually been incurred by the bank, from the point of view of strengthening the internal systems and controls and avoiding the possibility of such events turning into actual operational risk losses in future.

- Aside from information on gross loss amounts, banks should collect information about the data of the event, any recoveries, as well as some descriptive information about the cause/drivers of the loss event. The level of descriptive information should be commensurate with the size of the gross loss amount.

- Banks must develop specific criteria for assigning loss data arising from an event in a centralized function (e.g. information technology, administration department, etc.) or any activity that spans more than one business line.

- External loss data – Banks may also collect external loss data to the extent possible. External loss data should include data on actual loss amounts, information on scale of business operations where the event occurred, information on causes and circumstances of the loss events or any other relevant information. Banks must develop systematic process for determining the situations for which external data should be used and the methodologies used to incorporate the data.

- The loss data collected must be analysed, loss event category and business line wise. Banks to look into the process and plug any deficiencies in the process and take remedial steps to reduce such events.

Chapter 6

Controls / Mitigation of Operational Risk

6.1 Risk management is the process of mitigating the risks faced by a bank. With regard to operational risk, several methods may be adopted for mitigating the risk. For example, losses that might arise on account of natural disasters can be insured against. Losses that might arise from business disruptions due to telecommunication or electrical failures can be mitigated by establishing adequate backup facilities. Loss due to internal factors, like employee fraud or product flaws, which may be difficult to identify and insure against, can be mitigated through strong internal auditing procedures.

6.2 Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Both the Board of Directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a bank since such integration enables quick responses to changing conditions and avoids unnecessary costs. The bank should have a framework for testing the controls.

6.3 A system of effective internal controls is a critical component of bank management and a foundation for the safe and sound operation of banks. Such a system can also help to ensure that the bank will comply with laws and regulations as well as policies, plans, internal rules and procedures, and decrease the risk of unexpected losses or damage to the bank's reputation. Internal control is a process effected by the Board of Directors, senior management and all levels of personnel. It is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within the bank.

6.4 The internal control process, which historically has been a mechanism for reducing instances of fraud, misappropriation and errors, has become more extensive, addressing all the various risks faced by banking organizations. It is now recognized that a sound internal control process is critical to a bank's ability to meet its established goals, and to maintain its financial viability.

6.5 In varying degrees, internal control is the responsibility of everyone in a bank. Almost all employees produce information used in the internal control system or take other actions needed to effect control. An essential element of a strong internal control system is the recognition by all employees of the need to carry out their responsibilities effectively and to communicate to the appropriate level of management any problems in operations, instances of noncompliance with the code of conduct, or other policy violations or illegal actions that are noticed. It is essential that all personnel within the bank understand the importance of internal control and are actively engaged in the process. While having a strong internal control culture does not guarantee that an organization will reach its goals, the lack of such a culture provides greater opportunities for errors to go undetected or for improprieties to occur.

6.6 An effective internal control system requires that:

- An appropriate control structure is set up, with control activities defined at every business level. These should include: top level reviews; appropriate activity controls for different departments/divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorizations; and a system of verification and reconciliation.

- There is appropriate segregation of duties and personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimized, and subject to careful, independent monitoring.

- The three lines of defense (the first line of defense includes front office and business units, the second line of defense includes risk management and compliance and the third line of defense includes internal audit) exist and leverage on each other to manage and mitigate operational risks.

- There are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.

- There are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

- Effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

6.7 Adequate internal controls within the banks must be supplemented by an effective internal audit function that independently evaluates the control systems within the organization. Internal audit is part of the ongoing monitoring of the bank's system of internal controls and of its internal capital assessment procedure because internal audit provides an independent assessment of the adequacy of, and compliance with, the bank's established policies and procedures.

6.8 Operational risk can be more pronounced where banks engage in new activities or develop new products (particularly where these activities or products are not consistent with the bank's core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. It is incumbent upon banks to ensure that special attention is paid to internal control activities where such conditions exist.

6.9 In some instances, banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organization

and should be consistent with the bank's overall business strategy and appetite for risk. The bank's appetite as specified through the policies for managing this risk and the bank's prioritization of ORM activities, including the extent of, and manner in which, operational risk is transferred outside the bank. The degree of formality and sophistication of the bank's ORM framework should be commensurate with the bank's risk profile.

6.10 Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

- For all material operational risks that have been identified, the banks should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the banks should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely. Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies.

- Some significant operational risks have low probabilities but potentially very large financial impact. Classification of operational loss event into various risk categories based on frequency and severity matrix prioritize the events to be controlled and tracked. Audit benchmarks can be set for high loss events. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programmes can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain payout features, can be used to externalize the risk of " low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

- However, banks should view risk mitigation tools as complementary to, rather than a replacement for, internal operational risk control. Having mechanisms in place to quickly recognize and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools, such as insurance, truly reduce risk or transfer the risk to another business segment or area, or even create a new risk (e.g. legal or counterparty risk).

- Investment in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could transform high frequency-low severity losses into low frequency-high severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by external factors that are beyond the bank's immediate control. Such problems may cause serious difficulties for banks and could jeopardize an institution's ability to conduct key business activities. Banks should establish disaster recovery and business continuity plans that address this risk.

- Banks need to establish policies for managing risks associated with outsourcing activities, wherever considered necessary. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others, with greater expertise and scale, to manage the risks associated with specialized business activities. However, a bank's use of third parties does not diminish the responsibility of management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing bank. Furthermore, banks need to manage residual risks associated with outsourcing arrangements, including disruption of services.

- Depending on the scale and nature of the activity, banks should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. Banks should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the bank for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment. Banks should carry out an initial due diligence test and monitor the activities of third-party providers, especially those lacking experience of the banking industry's regulated environment and review this process (including re-evaluations of due diligence) on a regular basis. For critical activities, the banks may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

- Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption. These plans need to be tested annually and the plans may be revised to appropriately address any new or previously unaddressed parameters for these plans. For reasons that may be beyond a bank's control, a severe event may result in the inability of the bank to fulfill some or all of its business obligations, particularly where the bank's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in financial losses to the bank. This potential requires that banks establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of its operations.

- Banks should periodically review their disaster recovery and business continuity plans so that they are consistent with the banks' current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the bank would be able to execute the plans in the unlikely event of a severe business disruption.

Chapter 7

Independent Evaluation of ORM Function

7.1 The bank's Board of Directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate and effective system of internal controls, a measurement system for assessing the various risks of the bank's activities, a system for relating risks to the bank's capital level, and appropriate methods for monitoring compliance with laws, regulations, and supervisory and internal policies.

7.2 Internal audit is part of the ongoing monitoring of the bank's system of internal controls because it provides an independent assessment of the adequacy of, and compliance with, the bank's established policies and procedures. As such, the internal audit function assists senior management and the Board of Directors in the efficient and effective discharge of their responsibilities as described above. Banks should have in place adequate internal audit coverage to verify that operating policies and procedures have been implemented effectively. Board (either directly or indirectly through its Audit Committee) should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures.

7.3 The scope of internal audit will broadly cover:

- The examination and evaluation of the adequacy and effectiveness of the internal control systems and the functioning of specific internal control procedures.
- The review of the application and effectiveness of ORM procedures and risk assessment methodologies.
- The review of the management and financial information systems, including the electronic information system and electronic banking services.
- The review of the means of safeguarding assets.
- The review of the bank's system of assessing its capital in relation to its estimate of operational risk.
- The review of the systems established to ensure compliance with legal and regulatory requirements, codes of conduct and the implementation of policies and procedures.
- The testing of the reliability and timeliness of the regulatory reporting.
- Mitigating risks through risk-based audit.

7.4 All functional departments should ensure that the ORM Department is kept fully informed of new developments, initiatives, products and operational changes to ensure that all associated risks are identified at an early stage.

- Audit should periodically validate that the bank's ORM framework is being implemented effectively across the bank. To the extent that the audit function

is involved in oversight of the ORM framework, the Board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the ORM process. The audit function may provide valuable input to those responsible for ORM but should not itself have direct ORM responsibilities.

- Examples of what an independent evaluation of operational risk should review include the following:

    a) The effectiveness of the bank's risk management process and overall control environment with respect to operational risk.

    b) The bank's methods for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk.

    c) The bank's procedures for the timely and effective resolution of operational risk events and vulnerabilities.

    d) The effectiveness of the bank's operational risk mitigation efforts, such as the use of insurance.

    e) The quality and comprehensiveness of the bank's disaster recovery and business continuity plans.

Annexure 1

Broad Functional Roles within the Risk Management Structure

Note: *These are indicative in nature. Bank may add/modify as per its needs.*

1. Key functions of Risk Management Committee of Board (RMCB)

- Approve operational risk policies and issues delegated to it by the Board.
- Review profiles of operational risk throughout the organization.
- Approve operational risk capital methodology and resulting attribution.
- Set and approve expressions of risk appetite, within overall parameters set by the Board.
- Re-enforce the culture and awareness of operational risk management throughout the organization.

2. Key functions of Operational Risk Management Committee (ORMC)

ORMC is an executive committee. It shall have as its principal objective the mitigation of operational risk within the institution by the creation and maintenance of an explicit ORM process. The committee will be presented with detailed reviews of operational risk exposures across the bank. Its goals are to take a cross-business view and assure that a proper understanding is reached and actions are being taken to meet the stated goals and objectives of ORM in the bank. The committee may meet quarterly or more often, as it determines is necessary. The meetings will focus on all operational risk issues that the bank faces. Key roles of the committee are:

- Review the risk profile, understand future changes and threats, and concur on areas of highest priority and related mitigation.
- Assure adequate resources are being assigned to mitigate risks as needed.
- Communicate the importance of ORM to business areas and staff components and assure adequate participation and cooperation.
- Review and approve the development and implementation of ORM methodologies and tools, including assessments, reporting, capital and loss event databases.
- Receive and review reports/presentations from the business lines and other areas about their risk profile and mitigation programs.
- To monitor and ensure that appropriate ORM frameworks are in place.
- To proactively review and mange potential risks which may arise from regulatory changes/or changes in economic /political environment in order to keep ahead.
- To discuss and recommend suitable controls/mitigations for managing operational risk.
- To analyze frauds, potential losses, non-compliance, breaches, etc., and recommend corrective measures to prevent recurrences.
- To discuss any issues arising / directions in any one business unit/product which may impact the risks of other business/products.
- To continually promote risk awareness across all business units so that complacency does not set in.

3. Risk Management Department (RMD)

RMD in a bank is a critical function responsible for identifying, assessing, monitoring, and mitigating various risks that the business may face. Specific activities of RMD include:

- Regularly conduct risk assessments (credit risk, operational risk, liquidity risks, etc.) and analysis to identify both internal and external risks.
- Identify the overall risk appetite and risk tolerance of the bank with respect to various products and processes.
- Develop comprehensive risk management policies that align with the bank's risk appetite and regulatory requirements.
- Use quantitative and qualitative methods to assess risks, assigning values to potential losses and probabilities.
- Implement risk control measures, set risk tolerance levels, and establish internal controls to manage and mitigate risks effectively.
- Monitor and enforce compliance with relevant laws, regulations, audit findings and industry best practices.
- Provide regular risk reports, highlighting the current risk profile, emerging risks, and the effectiveness of risk mitigation measures.
- Establish and implement business continuity plans to ensure the bank's essential functions can continue in the face of disruptions.
- Provide training and educational programs to staff, at all levels, to enhance awareness of risks and risk management practices.
- Evaluate capital adequacy in relation to the level of risks faced by the bank and regulatory requirements.
- Conduct stress tests and scenario analysis to understand how the bank's financial position would be impacted under different stress scenarios.
- Periodic review and updation of the policy, risk appetite and risk thresholds as well as identifying new risks and implementing adequate control mechanism.

4. Key functions of Operational Risk Management Department (ORMD)

ORMD is responsible for coordinating all the operational risk activities of the bank, working towards achievement of the stated goals and objectives. Activities include building an understanding of the risk profile, implementing tools related to ORM, and working towards the goals of improved controls and lower risk. ORMD works with the operational liaisons within the business units, staff areas and with the corporate management staff. The group is organized within the Risk Management function. Specific activities of the ORMD include:

- *Risk Profile* – ORMD will work with all areas of the bank and assemble information to build an overall risk profile of the institution, understand and communicate these risks, and analyze changes/trends in the risk profile. ORMD will utilize the following four-pronged approach to develop these profiles:
    a) Key Risk Indicators (KRI)
    b) Risk and Control Self-Assessment (RCSA)
    c) Loss Database
    d) New product approval framework

- *Tools* – ORMD is responsible for the purchase or development and implementation of tools that the bank will use in its ORM program.

- *Consolidation and Reporting of Data* – ORMD will collect relevant information from all areas of the bank, build a consolidated view of operational risk, assemble summary management reports and communicate the results to the risk committees or other interested parties. Key information will include risk indicators, loss event data and self-assessment results and related issues.

- *Analysis of Data* – ORMD is responsible to analyze the data on a consolidated basis, on an individual basis and on a comparative basis.

- *Best Practices* – ORMD will identify best practices from within the bank or from external sources and share these practices with management and risk specialists across the bank as beneficial. As part of this role, they will keep up to date on rules and regulations, monitor trends and practices in the industry, and maintain a database/library of articles on the subject.

- *Advice/Consultation* – ORMD will be responsible for working with the risk specialists and the businesses as a team to provide advice on how to apply the ORM framework, identify operational risks and work on solving problems and improving the risk profile of the bank.

- *Insurance* – ORMD will work with the bank's insurance area to determine optimal insurance limits and coverage to assure that the insurance policies the bank purchases are cost beneficial and align with the operational risk profiles of the bank.

- *Policies* – ORMD will be responsible for drafting, presenting, updating and interpreting, the Operational Risk Policy.

- *Self-Assessment* – ORMD will be responsible for facilitating periodic self-assessments for the purpose of identifying and monitoring operational risks.

- *Coordination with Internal Audit* – ORMD will work closely with Internal Audit to plan assessments and concerns about risks in the bank. ORMD and Internal Audit will share information and coordinate activities so as to minimize potential overlap of activities.

5. Key function of Operational Risk Management Specialists (ORMS)

The bank-wide support departments (e.g., Legal, Human Resources, and Information Technology) shall assign a representative(s) to be designated as ORMS whose main responsibility is to work with ORMD and the departments/ businesses to identify, analyze, explain and mitigate operational issues within their respective areas of expertise. They will also act as verifiers for their related risks in the self-assessment process. They will accomplish this responsibility by involving themselves in the following:

- Committee Participation – ORMS shall be members of the committees and task forces related to ORM, as applicable. They must be ready to discuss operational issues and recommend mitigation strategies.
- Key Risk Indicators (KRIs) – Assist in the development and review of appropriate KRIs, both on a bank-wide and business specific basis for their area of specialty.
- Risk and Control Self-Assessment (RCSA) – Assist in the review of RCSA results and opine on the departmental/business assessment of risk types, quantification and frequency.
- Loss Database – Assist in the timely identification and recording of operational loss data and explanations.
- Gaps/Issues – Ensure that all operational risk issues are brought to the attention of ORMD and the department/business.
- Mitigation – Assist the department/business in the design and implementation of risk mitigation strategies.

6. Key functions of Business Operational Risk Managers (BORM)

It is expected that each business/ functional area will appoint a person responsible to coordinate the management of operational risk. This responsibility may be assigned to an existing job, be a full-time position, or even a team of people, as the size and complexity justify. Business/functional areas should determine how this should be organized within their respective areas. BORMs will report to their respective departments/businesses, but work closely with ORMD and with consistent tools and risk management framework and policy. ORMC will assure that these liaisons are appointed and approve their selection. The key responsibilities of the liaisons are:

- Self-Assessments – Will help facilitate, partake and verify the results of the self-assessment process.
- Risk Indicators – Design, collection, reporting, and data capture of risk indicators and related reports. Liaisons will monitor results and help work with their respective departments on identified issues. Resulting information will be distributed to both the departments and ORMD on a timely and accurate basis.
- Loss Events – Coordinate collection, recording and data capture of loss events within the businesses and regular reporting of these events, the details, amounts.
- Gaps/Issues – Responsible for the timely follow-up, documentation and status of action plans, open issues (Internal Audit, External Audit, Regulator and Inspector) and other initiatives waiting to be completed.
- Committee Participation – Must prepare to be called upon to attend ORMC meetings, when necessary, to discuss operational risk issues.
- Risk Mitigation – Responsible for consulting/advising the business units on ways to mitigate risks. Work with business areas and respective departments on risk analysis and mitigation.

7. Key functions of Department Heads

Business/functional area heads are responsible for risk taking, related controls and mitigation. They are ultimately responsible for implementation of sound risk management practices and any resulting impact for operational losses. To support this responsibility, they will have the following responsibilities related to ORM:

- Risk Ownership – The department heads shall take ownership of the operational risks faced in their departments/businesses.
- Understanding – Understanding the profile of operational risk facing the area and monitoring changes in the business and risk profile. Department heads may be expected to present their risk profiles and action plans to the ORMC.
- Risk Indicators – Collection and preparation of various risk indicator reports.
- Loss Events - Identification of loss events within the businesses and regular reporting of these events, the details, amounts and circumstances to ORMD on a complete and timely basis.
- Self-Assessment – Responsible for the periodic completion of self-assessments.
- Risk Mitigation – The businesses are responsible for developing strategies for the mitigation of risk where required (or managing those risks that are deemed to be acceptable).

Annexure 2

Business Lines Mapping and Loss Event Types

Table 1 - Mapping of Business Lines			
Business unit	**Business Line**		**Activity Groups**
	Level 1	**Level 2**	
Banking	Retail Banking	Retail Banking	Retail lending and deposits, banking services, trust and estates, etc.
		Private Banking	Private lending and deposits, banking services, trust and estates, investment advice, etc.
		Card services	Merchant/Commercial/Corporate cards, private labels and retail, etc.
	Commercial Banking	Commercial Banking	Project finance, real estate, export finance, leasing, lends, guarantees, bills of exchange.
	Payment and Settlement	External clients	Payments and collections, clearing and settlement.
	Agency Services	Custody	Escrow, depository receipts, securities lending (customers).
Others	Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, private equity, etc.
		Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, etc.
	Retail Brokerage	Retail Brokerage	Execution and full service.

Table 2 - Loss Event Type Classification			
Category (Level 1)	**Definition**	**Category (Level 2)**	**Category (Level 3)**
Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.	Unauthorised activity	• Transactions not reported (intentional) • Transaction's type Unauthorised (monetary loss) • Mismarking of position (intentional)
		Theft and Fraud	• Fraud/credit fraud/worthless deposits • Theft/extortion/embezzlement/ robbery • Misappropriation of assets • Malicious destruction of assets • Forgery, Check kiting, • Smuggling • Account takeover/ impersonation/etc. • Tax non-compliance/ evasion (wilful), Bribes/kickbacks Insider trading (not on bank's account)
External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	Theft and Fraud	• Theft/robbery • Forgery, check kiting
		Systems Security	• Hacking damage • Theft of information
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discriminatio n events.	Employee Relations	• Compensation, benefit • Termination issues
			• Organized labour activity • General liability (workplace accidents, slip and fall, etc.) • Employee health and safety rules events • Workers' compensation
		Diversity and discrimination	• All discrimination types
Clients, Products and Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary & suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	• Fiduciary breaches/guideline violations • Suitability/disclosure issues (KYC), etc. • Retail consumer disclosure violations • Breach of privacy • Aggressive sales • Account churning • Misuse of confidential information • Lender Liability
		Improper Business or Market Practices	• Antitrust • Improper trade/market practices • Market manipulation • Insider trading

Table 2 - Loss Event Type Classification			
Category (Level 1)	**Definition**	**Category (Level 2)**	**Category (Level 3)**
			• Unlicensed activity • Money laundering
		Product flaws	• Product defects (Unauthorized, etc.) • Model errors
		Selection, Sponsorship & Exposure	• Failure to investigate client as per guidelines • Exceeding client exposure limits
		Advisory Activities	• Disputes over performance of advisory activities
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disasters or other events	Disasters and other events	• Natural disaster losses • Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	• Hardware • Software • Telecommunications • Utility outrage/disruptions
Execution, Delivery & Process Management	Losses from failed transactions processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution Maintenance	• Miscommunication • Data entry, maintenance or loading error • Missed deadline or responsibility • Model/system misoperation • Accounting error/entity attribution error • Other task misperformance • Reference data maintenance
		Monitoring and Reporting	• Failed mandatory reporting obligation • Inaccurate external report (loss incurred)
		Customer intake and documentation	• Client permission • Client permissions/ disclaimers missing • Legal documents missing/ incomplete
		Customer client account management	• Unapproved access given to accounts • Incorrect client records (loss incurred) • Negligent loss damage of client assets
		Trade Counterparties	• Non-client Counterparty misperformance
		Vendors & Suppliers	• Outsourcing • Vendor disputes

Annexure 3

Risk and Control Self-Assessment (RCSA) Framework

1. Objective:

- To assist ORMD to identify and assess major operational risks on a regular basis.
- To identify inherent and residual levels of the risks.
- To assist the bank in ascertaining whether appropriate controls are in place and operating.
- To facilitate in formulating an action plan for mitigation of operational risk and reduction of control gaps.
- To assist in generating reports on the overall risk control in the bank.
- To formulate the basis for risk and control assessments.
- To review the control gaps & action plan at quarterly intervals & update RCSA register at annual intervals.

2. Key elements:

- RCSA is a bank wide exercise which may conducted annually and reviewed periodically by the Board.

- RCSA register is to be maintained by the bank wherein concerned product/process of the concerned departments, risk applicable thereof, control measures to be adopted are identified, described and rated. The control gaps and action plans of the RCSA register needs to be reviewed quarterly but the RCSA register itself needs to be reviewed annually. While reviewing and updating the RCSA register, due diligence needs to be exercised by the Board and senior management in identifying the new risk, control gaps and the remedial mechanism.

- Scope of the RCSA register is summarized below:
  a) Identification and assessment of the inherent risk.
  b) Identification and assessment of control mechanism
  c) Assessment of residual risk.
  d) Generation of Health index.
  e) Reporting of the RCSA results.
  f) Periodic updation and review of the gaps and progress of action plan.

3. Steps for RCSA exercise

a) Identification of products, process and sub-processes - The first step is the identification of the products/ process or sub-processes associated with the RCSA unit (HO departments, Regional Offices, branches or bank as a whole). E.g., in Credit Department, 'Housing loan' is a product and 'Appraisal', 'Documentation', 'Monitoring', etc., are the processes involved and sub-process may be 'Client appraisal', 'KYC compliance', etc. Similarly, in HR department 'Training' is a product and process would be 'Training policy', 'Conduct of training need analysis', 'Preparation of training calendar', etc.

b) The products, processes and the sub-processes may be mapped to the business line. (Refer **Annexure 2, Table 1**).
c) Identification of the inherent risk- Inherent risks mean the risk as it stands assuming there is no control to mitigate it within the RCSA unit that may be associated with people, process, system and external events. In creating a RCSA register, the process, the sub-process, and the inherent risk are described. To arrive at the inherent risk, one may use judgement of the impact category that a failure in any process/sub-process can lead to. For example, in case of an inadequate check on KYC of customer before approving a loan facility, it is possible that a regulatory violation is committed, leading to regulatory risk or in case of 'Credit appraisal' of the loan, the inherent risk that can arise are wrong project selection, improper internal credit rating, wrong valuation done, etc.
d) The inherent risk may be classified based on "loss event type" as mentioned in the **Annexure 2, Table 2.**
e) Risk owner may be defined for each risk. Accountability should be properly documented.
f) The 'type of impact' for each inherent risk should be mentioned (legal/compliance impact, financial impact, reputational impact, environmental impact, customer impact, etc.). E.g., non-compliance of KYC-AML can cause regulatory impact, lower credit rating from the higher financing authority may have reputational impact.
g) Assessment of risk - Assessment is made based on the probability and severity of the risk events. Scores may be given from 1-5 in ascending order to define the probability and impact of the events. E.g., high probability high impact events will be marked 5 each.

Illustrative chart for probability and severity is given below.

I. Scale for rating probability (Banks may devise according to the size and complexity of the organisation) –

Likelihood	Description	Score
Rare	<10% chance of occurrence Once in 2 years or more	1
Unlikely	10-35% chance of occurrence Once in a year.	2
Possible	35-65% chance of occurrence Once in a quarter.	3
Likely	65-90% chance of occurrence Once in a month.	4
Frequently	>90% chance of occurrence Once in a week or more.	5

II. Scale for rating impact/severity. (The figures and scenarios mentioned below are illustrative in nature. Banks may devise the same according to the size, complexity and area of operation, etc.)

Severity	Scenario	Score
Very Low	Financial loss less than Rs. 1 lacs **OR** Local reputational loss **OR** .etc.	1
Low	Financial loss between Rs. 1 lacs to Rs. 5 lacs **OR** Regional negative media coverage reputational loss **OR** etc.	2
Medium	Financial loss between Rs. 5 lacs to Rs. 10 lacs **OR** National short term media coverage reputational loss **OR** etc.	3
High	Financial loss between Rs. 10 lacs and Rs. 1 crore **OR** Local reputational loss **OR** etc.	4
Very High	Financial loss more than Rs. 1 crore **OR** International/ national long term media coverage **OR** etc.	5

h) Inherent risk rating and evaluation - The overall risk rating is arrived at by multiplying the probability score and the impact score as mentioned in the section 'g. Assessment of Risk.' The minimum risk rating for an inherent risk would be 1 and maximum rating would be 25. After the rating is calculated, evaluation is to be done based on the criteria fixed by the bank. Illustrative evaluative table is given below for reference (Banks may devise according to the size and complexity of the organisation).

Sl no.	Score	Inherent Risk
1	< or = 3	Insignificant
2	4-6	Moderate
3	7-11	Medium
4	12-15	High
5	>15	Extreme

For example, if the probability of the event is once in a month, then the probability score is 4 and if the financial loss bank may suffer is Rs. 8 lacs, then the impact score is 3. The total inherent risk score is 4x3=**12.** Based on such score, the overall inherent risk of the bank is **High.**

i) After the evaluation, the next step is to identify the specific control mechanisms and control owner to mitigate the inherent risks. E.g., constitution of committees, review of policies, audit, technological measures, etc.

j) Assessment of the overall control mechanisms – The overall control mechanism is rated based on the score of control design effectiveness and control operating effectiveness.

I. Control design effectiveness – It depicts whether the control is manual driven or IT driven or both and whether it is preventive in nature or detective in nature. An illustrative scoring is given below. (Banks may devise according to the size and complexity of the organisation)

Design effectiveness		Score
Only manual controls without maker/checker control	Risk mitigation only through detective/ corrective measures.	1
Partially automated without maker/checker controls	Risk mitigation mostly through detective/ corrective measures.	2
Manual controls with manual maker/checker controls	Risk mitigation through partly preventive but mostly detective/ corrective measures	3
Partly automated with maker/ checker details or audit trails	Risk mitigation mostly through preventive but partly detective measures	4
Fully automated with maker/ checker and audit trails	Risk mitigation through mostly preventive measure	5

II. Control operating effectiveness – The effectiveness of the existing controls in the bank can be assessed by making use of the existing testing framework in the bank, e.g., concurrent audit observations, Inspection Department's observations, etc. The scoring of the control operational effectiveness can be based on the frequency of the control lapses or exceptions occurred testing framework. An illustrative scoring is given below. (Banks may devise according to the size and complexity of the organisation)

Control Effectiveness	Score
Control lapses occurred more than twice in the last 3-6 months	1
Control lapses occurred twice in the last 3-6 months	2
Control lapses occurred once in the last 3-6 months	3
Control lapses observed once in the last 12 months	4
No incidents of control lapses in last 12 months	5

k) Overall control effectiveness: This is the product of control design and the control effectiveness. Maximum score is 25 and minimum is 0.

An illustrative evaluation table is given below. (Banks may devise according to the size and complexity of the organisation)

Score Range	Overall Control effectiveness
0-5	Significant improvement needed
>5-10	Improvement needed
>10-15	Meets requirement
>15-20	Effective control present
>20-25	Significantly effective control

l) Residual risk and evaluation: Residual risk is the one which is not eliminated after installing all the control mechanism in place. E.g., cyber-attack from an unknown source although the chances of such occurrence were significantly reduced. Lower the control effectiveness, higher the residual risk and vice versa. Evaluation of the residual risk is made by dividing the inherent risk score by the overall control effectiveness score and finding the criticality from the below table. The table given below is

illustrative in nature and banks may devise according to the size and complexity of the organisation.

Residual Risk	Interpretation
0.01 - 0.60	Low
0.61 - 1.70	Medium
1.71 - 4.44	High
=> 4.45	Significant
N/A	No control

m) Implementation of Action Plan: Whenever any residual risk scores of risk events are found to fall in the 'High', 'Significant' and 'No Control' zone, an action plan must be documented for appropriate and prompt corrective and preventive action. Any risk factor that is not currently controlled effectively is to be identified by the relevant RCSA unit for initiating corrective and preventive action. The additional control mechanism or step wise action plan required to mitigate the residual risks may be identified and indicated. Additional control mechanism may consist of putting in place 'Standard Operating Procedures' in case these do not exist, enhancing capacity building of staff, posting of additional staff, digitization of records in case of manual procedures (wherever applicable), or any other system or possibility if there is 'no' additional control mechanism required for mitigating a particular residual risk. The corrective action plan may include the following: clear description of each control's weakness; action plan to resolve the deficiency; Officials responsible for implementing and monitoring the implementation of the action plans; target date for resolution/ timelines for implementation of the action plan. Any slippage in meeting previously agreed target dates must be documented in the RCSA data summary.

n) Control Testing Requirements: For risk events where control gaps have been mitigated by issue of fresh instructions/ guidelines to improve the existing control, testing would be performed on a periodic basis. The initial testing for controls (improved/ new) should be performed by an independent officer (other than the official who performs the underlying work or is involved in monitoring of that control activity). This testing can be carried out on a selected sample of RCSA units. The testing activity would be initiated by Risk Coordinators/ Risk Managers/ Nodal Officers and the test results shall be maintained by RMD for monitoring of the suggested action plans. In case RMD concludes that the test results are satisfactory (i.e., test results showing that the control, for a revised process or after mitigation of control gaps, is operating effectively) the same shall be incorporated in the Internal Audit Plan. However, in case the control is not operating as desired then the exercise is to be performed for those controls every six months by the Risk Coordinators and Risk Managers. Testing procedure should ensure high degree of assurance in higher risk areas. When changes occur in the business environment (e.g., new controls being implemented, new roles being assigned for existing controls, etc.), systems (e.g., implementing new systems, manual or IT) or system outputs (e.g., generation of new system reports, etc.), RCSA unit and Risk Coordinators/

Risk Managers/ Nodal Officers, under the guidance of RMD may ensure that the testing covers these changes and verifies that the controls are still working properly. The testing results shall be presented by RMD to top management/committees.

o) Monitoring RCSA results: Board/ top management committee shall monitor the identified process gaps and corresponding action plans and shall review these plans till completion/ resolution. RCSA units, with high residual risk rating and units whose risk and control score are considerably different from the one arrived by majority of the units, need to be prioritized for monitoring and resolution.

p) Report RCSA results: RMD shall discuss the test results with the concerned Risk Coordinators and report the same to Board/top management committee as required. RCSA unit level data needs to be submitted by Risk Managers/ Risk Coordinator of RMD as per the proposed template. (RCSA register). RCSA data summary would be incorporated into the comprehensive Operation Risk Report by RMD which may include the following: RCSA units' health index, RCSA units by residual risk level, RCSA units by control rating, RCSA units with significant difference in the residual risk rating and the control rating as compared to other units, etc.

RCSA Register Template (Illustrative)

Risk No.	Product	Process	Sub-Process	Business line mapping	Inherent Operational risk	Loss event type	Risk Owner
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)

Frequency of the activity	Type of impact	Probability	Severity	Inherent Risk Rating & Evaluation	Control description	Control Owner	Control Frequency
(9)	(10)	(11)	(12)	(13) = [12x11]	(14)	(15)	(16)

Manual/ IT and Preventive/ Detective	Control Design (Manual/ IT and Preventive/ Detective) – Rating	Control Operating Effectiveness	Control operating effectiveness rating	Overall Control score	Overall control Rating	Control Gap	Residual Risk rating
(17)	(18)	(19)	(20)	(21)=[18x20]	(22)	(23)	(24) = [13/21]

Residual risk level	Recommendation	Action Plan	Person responsible - Implementation	Person responsible - Monitoring	Timelines
(25)	(26)	(27)	(28)	(29)	(30)

4. Assigning Health Index:

Health index is the indicator of the level of operational risk existing in an RCSA unit. Overall “Health Index” for a RCSA unit would be calculated by aggregating the

weighted residual risk score (in section 'l. Residual risk and evaluation' above) of all risk events in the RCSA unit. The results of the RCSA exercise are used to compute health index.

Approach for calculation is as follows:

I. It is necessary to provide appropriate risk weights, depending upon the criticality of risk, to arrive at overall health index of the bank.

II. Accordingly, the residual risk shall be assigned a risk weight depending upon their criticality. A higher residual risk shall be assigned a higher weight and so on. Each of the residual risk buckets would be assigned a weight for aggregation of the results. e.g., "Significant' and "No Control" would have higher weights and a reduction in the weights till we move to 'Low' bucket.

III. Overall "Health Index" for an RCSA unit would be calculated by aggregating the weighted residual risk score of all risk events in the RCSA unit. E.g., health index for Head Office of the bank would be the aggregation of all the risks of all HO departments.

IV. Health Index Rating for RCSA unit and the bank as a whole must be presented to top management committee/Board on an annual basis. The calculation of the same shall be carried out by RMD, based on the results of RCSA.

V. Sample "Health Index" calculation for reference is given below:

Risk weight may be assigned as mentioned below or as may be decided by the management of the bank.

Low	Medium	High	Significant	No Control
1%	40%	70%	90%	100%

Below mentioned is the Health index computation of the Head Office RCSA unit. The risks associated with each department are identified in columns 2 to 6.

Operational Risk Health Index									
Dept	Low	Medium	High	Significant	No control	Total (weighted)	No. of Risk	Risk Index	Health Index
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
						[1%*(2)] + [40%*(3)] + [70%*(4)] + [90%*(5)] + [100%*(6)]	(2) + (3) + (4) + (5) + (6)	(7) / (8)	[100 – (9)]
HR	6	13	4	2	3	12.86	28	46%	54%
Credit	5	12	5	1	1	10.25	24	43%	57%
FD	0	20	8	5	1	19.1	34	56%	44%
IT	0	15	4	2	5	15.6	26	60%	40%
Total	**11**	**60**	**21**	**10**	**10**	**57.81**	**112**	**52%**	**48%**

The health Score arrived at is further categorized into the four-point health index tabulated as below:

Sl. No.	Health Index	Category
1	=> 80%	Low risk
2	< 80% and => 60%	Medium Risk
3	< 60% and = >40%	High Risk
4	< 40%	Significant Risk

In reference to the above example, the health index of the bank (48%) can be categorized as "High Risk".

Annexure 4

Key Risk Indicator (KRI) framework

1. Objective:

- To provide effective monitoring tool to track changes in risk levels and keep management apprised of shifts in established patterns.
- To quantify the operational risk appetite of the bank, wherever applicable.
- For timely reporting of significant control slippages.
- To minimize the occurrence of a risk event/ loss.
- To provide a monitoring tool that can give the bank a complete view of its operational risk.

2. Applicability:

This framework is issued in furtherance of the implementation of ORM policy of the bank. The framework will be applicable to all departments of Head Office, as well as Regional Offices and any other establishments (including Training Establishments) of the bank.

3. Approval and Review:

KRI framework and guidelines may be reviewed by RMCB. The results may be reviewed annually or as may be decided by the Board.

4. Key Terms:

- Key Risk: An event which can disrupt the entity's ability to implement the strategy or achieve its overall objectives hence increasing the operational risk.

- Key Risk Indicator (KRI): KRIs are early warning signals (EWS) in the form of statistics or metrics, which enable the management to monitor and mitigate the operational risk that exceed the acceptable levels. The bank's departments should perform an exercise to identify KRIs and should document the same. The same should be periodically updated by the respective departments or units and the same is reviewed by RMD.

- Risk Driver: Risk drivers are those factors that increase the probability of a risk materializing. The greater the number and complexity of risk drivers for a particular type of risk, the greater the potential for occurrence of a risk event. Examples are volume of transactions (i.e., an increase in business volume may lead to an increase in operational risk faced by the bank), manual processes (i.e., errors due to manual processes may lead to increased operational risk as compared to automated processes), new technology (introduction of new technology or processes may lead to increase in operational risk faced by the bank), etc.

- Threshold Level: This level is a measure which determines the seriousness/ probability of a risk materialising. Thresholds determine how well the bank's

operational activities are managed. These thresholds also demonstrate the risk tolerance of the activity/ operation. Threshold levels can be measured at three levels namely, green, amber and red (varying from acceptable level to unacceptable level) for each KRI. The color coding is to facilitate the attention of the management to the areas which are crucial.

a) Red: Highlights the need for immediate resolution
b) Amber: A potential problem which requires further review and analysis
c) Green: No immediate concern

For critical/ zero tolerance indicators, there would be only two zones, i.e., 'Red and Green'. For example, KRIs related to critical areas (regulatory penalties, occurrence of frauds, down time for critical systems, etc.) may be classified as critical/ zero tolerance indicators.

Risk tolerance is linked to the threshold limits set for each indicator, indicating that beyond the threshold, management action needs to be initiated. Hence risk tolerance refers to the risk bearing capacity of the bank and it can be defined in multiple ways and also at various levels. The methodology for calculation of tolerance levels is described in section 'Threshold determination and calibration' as mentioned below in this framework. Examples of tolerance limit are number of hours of downtime the bank can tolerate for critical IT systems, percentage of group/single borrowers for which the current exposure is close to 90% of the maximum limit, etc.

- Preventive / Lead Indicator: These are KRIs that indicate increased probability of the occurrence of a risk/loss event and are useful in initiating preventive measures. Using staff turnover as a simple example, this indicator would measure the risk of processing errors by employees who are fairly new to the task, especially in specialized areas like treasury, credit appraisal, etc. A preventive KRI would be tracking the number of key personnel who have not undergone training or having a maker/checker for all transactions. An employee earlier handled on an average 2 loan/ grant proposals in a week; due to business growth, the employee now handles 4 loan/ grant proposals during the same period. The increase in volume without a corresponding increase in manpower would imply that an employee may be required to skip some essential steps/ parts of the process so as to complete the increased volume within the same time period. Thus, percentage increase in the business without appropriate increase in manpower is a leading indicator of potential errors in the process.

- Detective/Lag Indicator: Theses are triggered once the risk/ loss event occurs. For example, percentage of cases that are pending for conduct of pre-disbursement activities (such as security creation) has exceeded the approved timeline; number of frauds which have occurred in the reporting period is a lag indicator of the occurrence of fraudulent activity in the bank; percentage of client complaints is a lag indicator of the level of customer satisfaction.

5. KRI Process Flow

- Identification of Key Risks: KRIs may be identified by the banks using the following illustrative criteria:
  a) Inherent risks identified in the RCSA exercise in 'Extreme' category and in addition, selective risks in the 'High' category may be considered.
  b) Control deficiencies identified during the RCSA exercise also serve as a base to identify KRI. Risks which have 'No Control' may be considered, while risks with residual risk rating of 'Significant' may also be considered for identification of KRIs.
  c) Key Performance Indicators (KPIs): If KPIs are not achieved frequently by the respective departments/RO/branch, it would indicate presence of underlying key risks that need to be identified and monitored by the bank.
  d) From observations of Inspection/ Audit.

  The identification of key risks is an ongoing process and risks identified are reviewed periodically for their relevance to the bank due to changes in people, processes, technology and introduction of new products. KRI template (illustrative) for identifying and monitoring KRIs is enclosed below.

KRI Template

Risk Description	KRI Description	Measurement Unit	KRI Nature	Source Data	Benchmark threshold	KRI value	Remarks	Criticality
1	2	3	4	5	6	7	8	9
The risk for which the KRI is developed	Detailed description to be provided.	Unit to be provided. Can be in numbers or %age.	1.Preventive 2. Detective	Source of data from where KRI value is obtained.	Threshold for 3 zones (can differ for various items) Red - R Amber - A Green - G E.g.R>15%, 10% < A <= 15%, G <= 10 %	Actual KRI value to be mentioned here. Can be in numbers or %age.	Any other remarks by the dept.	Is KRI to be reported in the current reporting period. (Yes/No)
Example:								
Non completion of pre-disbursement activities before giving loan	% of cases where post-sanction / pre-disbursement documents/ agreements are due but have not been collected for disbursed loans	%age	Preventive	CBS/inspection observation	•R>15%, •10%<A<= 15%, •G <= 10 %	% of cases where the documentation is not done before disbursement.	-do-	Yes

- Mapping Key Risks to Indicators: The ability to map key risks to their causal components such as risk drivers, processes, products and systems, both internal and

external to the bank, would have an improved understanding of why errors are occurring.

KRI for each of the identified risk would be drawn from risk drivers as indicated in the illustration below:

Sl. No.	Process	Sub-Process	Risk	Drivers
1	Pre-Sanction	Document verification	KYC details not obtained	Officers are not trained. Lack of circulars, procedures notes, etc.
				KRI: % of the bank's officers yet to be trained in document verification. % of cases where KYC has not been done, necessary security/ documents have not been collected from the borrower.

This selection can be modified over a period of time based on the bank's experience of whether KRIs have been demonstrating a reasonable predictive power, i.e., for a process where additional controls have been introduced, the results of KRI is following a downward trend, say movement from 'amber' zone to 'green' zone. This implies that KRI adequately reflects the risk profile and it can be concluded that this KRI has a reasonable predictive power. On the contrary, if the KRI result is 'green' while the RCSA or/and loss data observations are adverse, it implies that KRI is not designed correctly or threshold values are not set correctly and the respective KRI needs re-assessment.

- Threshold Determination and Calibration: Establishing limits is important to develop corrective mechanism for process owners and escalation to top management, when warranted. The process of setting the thresholds is an ongoing process which includes defining the thresholds, collecting data and analysis of the data to check for results as to whether they accurately reflect the risk. For example, if majority of the indicators are in the red/amber zone, though the values of the indicators are in not showing major variation with historical values in the bank, it would be an indication that the calibration of thresholds needs to be relooked at. This would necessitate recalibration of thresholds, the effectiveness of which (new thresholds) would be monitored in the next KRI reporting cycle.

  Initially, the thresholds would be set up as follows:

  a) Based on historical data: For example, in case business departments have historical data to suggest loan delinquencies for 5 days is acceptable and is not a cause for concern, the 'green' indicator may be set at 5 days. Any breach beyond this level may be classified under the 'amber or red zones'.
  b) Based on Management's Estimation (experience over time): This is in the absence of any historical data. In the example quoted in the above para, in the absence of data on loan delinquencies, if past experience has indicated that loan delinquencies within 5 days is acceptable or normal, then the 'green' indicator may be set at 5 days and so on.

- KRI Reporting: KRIs should be reported by the departments on an annual basis to RMD. The report should consist of detailed KRI status prepared by the Risk

Coordinators/ Risk Managers highlighting the issues at the Head Office department, Regional Office, branches and other establishment levels. An illustrative reporting format is given below.

KRI description	Benchmark threshold	KRI value observed	Comments	Action taken
For example - No. of frauds detected during the period	Red (1 and above) Amber (0) Green (0)	1	Detected no. of fraud is 1. Hence, KRI is in Red zone.	E.g., system controls are made more stringent.

- KRI Testing: The testing can be done according to the judgement of the RMD/Risk Managers/ Risk Coordinators. A few ways of testing is given for the reference of the banks:
  a) KRIs that have been reported as green/ amber for a consecutive period of six months may be tested to identity any misreporting.
  b) KRI reported "green' in spite of adverse audit findings/ loss occurrence may also be considered for identification of misreporting.
  c) Monthly operations reports/ Transaction reports, statutory auditors/ inspection/ CAC reports and any other report/ findings should be used to ascertain whether the reporting of KRI has been done correctly.

- Escalation and Monitoring: RMD may analyze adverse KRIs based on threshold values and notify the respective HO departments, Regional Offices, branches and other establishments. The action points originated from the escalation to be documented and tracked by RMD to reduce any possible loss to the bank.

- Re-Assessment of Indicators and Thresholds: Identification of KRI and assessment of the thresholds is an ongoing process. In case a certain process has been materially redesigned, or the controls have been altered, historical data will be of limited value. Hence, assessments need to be conducted continuously to evaluate the relevance of risks, controls, risk drivers and KRI.

  RMD may evaluate the relevance and efficiency of the KRI on an annual basis, with a view to maintain and improve the quality of risk indicators. RMD, in consultation with business departments/reporting units may eliminate KRIs which are not capable of reflecting the true picture. Documentation of reasons for eliminating or revising KRIs should be maintained. For example, an existing KRI relating to a specific process that was earlier performed in-house, which is now outsourced, is less relevant today. A different KRI would be needed to have a check on the quality of outsourcing.

Annexure 5

New Product Approval Framework

1. Objective

To ensure that,

- All risk aspects are considered before the product/ process is launched, and that product features are designed/ modified to mitigate identifiable risks.
- The approval for new products/ processes are being made by a competent authority.
- The product process meets all regulatory requirements.
- A framework is put in place to prevent losses, due to possible frauds and process flaws, through adequate risk mitigation measures suggested by the support departments or any designated committee.
- The product/process is thoroughly understood and reviewed by all the concerned departments.

2. Applicability

All departments in HO & branches, and other establishments should follow the framework as laid by the bank.

3. New Product / Process

A product / process is considered new, if it meets any of the following criteria:

- New to the bank though existing in the marketplace.
- It is new to the marketplace and has not been introduced by any other financial institution so far.
- The product has remained dormant for a defined period, e.g., one or more year/s, and is being re-launched.
- An existing product getting revised now subject to change in regulation or policy with additional new features.

4. Framework Exclusions

Matters related to pricing, limits, exposure norms and capital allocation in respect of new products shall be considered by the appropriate committee/s as setup by the bank and shall be beyond the purview of this framework.

5. Product Scrutiny Committee (PSC)

PSC should be formed within the RMD. The bank may decide the composition of the committee to suit their size and complexity. Apart from the members of the RMD, relevant officials from concerned proposing department may be made part of the committee meetings. The role of the committee is to recommend / reject / defer new products / processes proposed by the proposing department/s, with or without any modifications.

6. Role of the Proposing Department

- Develop the initial concept of the respective new product / process and prepare the Product Note (PN), to seek PSC recommendations prior to launch of the proposed product / process.
- Forward the PN to the convener of the PSC meeting for scrutiny.
- Coordinate among various support departments for review of product / process.
- Incorporate the changes recommended by PSC in the new product / process.
- Address any queries or clarifications raised on the PN.

Whenever new products/processes are to be introduced, the concerned department shall prepare a PN, containing details such as the summary of the product/process, key features and process flow with responsibilities, system requirements, regulatory compliance, accounting and taxation issues, the applicable risks, operational risk mitigation measures, compliance risk mitigation measures, credit risk mitigation measures, market risk mitigation measures and any other matter which the bank decides to detail further.

The convener of PSC shall circulate the PN at least 5 working days, or at an interval as per the need of the bank, before the PSC meeting.

7. Conduct of PSC meeting

Conduct of PSC meeting shall be done by RMD (Operational Risk vertical). All the members to be informed well beforehand and all the documents to be circulated prior to the meeting of PSC to discuss and deliberate upon the new products/ processes proposed. The PSC may, after due deliberation:

- Recommend the PN without any change.
- Recommend PN with modification as may be decided by the members PSC.

8. Annual review and modification

Annual review may be carried out by the concerned department and to be reported to the head of the department.

Annexure 6

Incident and Loss Management Framework

1. Objective

- Establishing a process for timely and immediate reporting of incidents.
- Minimizing the future recurrence of similar loss events, by identifying control weaknesses in identified losses.
- Meeting the loss data collection standards as required by the regulator.

2. Incident and Loss Reporting Process

An operational risk event is defined as inadequate and failed internal processes, people and / or systems or external events causing any of the following adverse impact:

- Events constituting actual loss.
- Events with future impact (near miss).
- Events without loss (or gain).
- Events which seriously jeopardise the business operations.
- Events caused/causing threat to employees' life, etc.

Examples of operational risk events are breach of trading limits, sanction/ disbursement to ineligible clients due to inadequate procedures, cyber-attacks/ system downtime leading to disruption in the bank's critical business operations, all of which may lead to losses or near misses.

The process is as follows:

3. Incident Reporting & Management

- Concerned staff official in the HO department/RO/branch/other establishment should report to the respective Department Head, Risk Manager or Risk Coordinator of any incident, which has resulted in an operational loss/near miss/ event with gain, etc., within 24 hours of such occurrence. In case a third party/ vendor observes any incident, and the same is brought to the notice of a staff member/ Risk Manager, such incidents may also be reported as per the procedure outlined in the following paragraphs.
- The concerned HO department/RO/branch/other establishment may report the incident as per the Loss Data Template defined by RMD (template should contains details of the event, amount of loss incurred, time of incidence, accounting entries, recovery, etc.). Thereafter, the concerned Risk Coordinator shall validate all the fields, follow up for obtaining requisite information, if any, and report the completed loss data form to RMD, HO within 48 hours, after due approval by the concerned Head of the department or Officer in charge of the unit.
- However, in case of incidents having potential of turning into a disaster, such incidents may also be reported to the appropriate authority, as soon as possible.
- Based on the details indicated in Loss Data Template, RMD shall undertake further analysis of the reported event as per the Loss Data Template.

Operational loss events may be reported under various Loss Event Types as per **Annexure 2 Table 2**.

- Thereafter, the concerned HO department/RO/other establishments may initiate necessary corrective action to minimise the operational loss, if any, and to recover any amount due to the bank. The details thereof may be incorporated under the Loss Data Template.
- Thereafter, details of loss data along with the recovery details may also be captured under in Loss Data Template.
- The concerned HO department/RO/branch/other establishments may initiate efforts to recover the full loss (cash outflow) from the party which was the inadvertent beneficiary. Recoveries may be in the form of direct cash recovery in full in one lump sum or in parts, either by way of an insurance claim or through any other mode, as applicable.
- In case the loss amount is partially recovered by the time the incident is reported, the reporting unit may enter the details (loss and recovery) in the Loss Data Template and forward the same to the concerned Risk Coordinator and Risk Manager.

4. Root Cause Analysis

- The reporting department/RO/branch/other establishments may undertake a detailed root cause analysis, identify/ analyse the causes of the incident, assess the design and effectiveness of the controls and summarise the lessons learnt for all reported events. The concerned Risk Coordinators and Risk Managers may facilitate the HO department/RO/branch/other establishments in identifying the root causes and framing the lessons learnt.
- Template for undertaking root cause analysis is to be framed by RMD and the same is to be used by the reporting department for documenting root cause analysis.
- Similarly, the issue & action plan for remedial action may be prepared as per the format prescribed by the RMD.

5. Incident Closure

- Issue & action plan for remedial action may be prepared and the same is to be followed up by the reporting department. RMD should carefully review and oversee whether the compliances for the action points are met.
- The closure of the loss record implies that the loss amount recorded is final and that recovery, if any, has been recorded against the loss incurred. There may be instances where the final loss amount has been recorded but the case has not been closed (e.g., in litigation matters or in complex events where additional time for investigation or repair is required). The concerned HO departments/RO/branch/other establishments may track all 'open' cases to ensure that the progress towards resolution is made within the mutually agreed timeline between the concerned department/RO/branch/other establishments and RMD. These details will also be captured in Loss Data Template and the status of 'open' cases may be reviewed by RMD on a quarterly basis.

6. Accounting

- Operational risk losses may be accounted once the loss amount is crystallized and has been validated by the validator (concerned Risk Coordinator). A detailed accounting procedure for booking operational risk losses may be implemented by the bank.
- The process flow for accounting procedure shall be as follows: Once the loss amount has been recognised as either a write off (confirmed loss), provision (loss amount yet to be realized) or recovery amount, and after adequate approvals have been sought, the concerned department may be advised for passing necessary accounting entries.
- Prior to the annual closing exercise, the accounting entries/balances, the write off amount and the net loss may be reconciled against the individual entries in the operational risk loss database, for any discrepancies if any, between the operational risk loss database and the bank's accounting system may be documented; irrespective of the amount and/or stage of recovery, all incidents have to be accounted for. In the case of recoveries, accounting entries to be passed by the reporting unit responsible for accounting of losses.
- Reconciliation of the closed loss records may be done by RMD and communicated to the concerned department and pass necessary entries as applicable.

7. Retention of data

RMD may decide on how long the loss data is to be maintained.

*****