NCC Bank
नेपाल केडिट एण्ड कमर्स बैंक लि.
Nepal Credit & Commerce Bank Ltd.

Administration Circular No: 55/2016

Date of Issue: December 16, 2016
(Poush 1, 2073)

Subject: Operational Risk Management Policy & Framework 2016

To: All the Staff Members of Nepal Credit & Commerce Bank Ltd.

This is to inform all the staff members of NCC Bank that the Management Committee (Board) Meeting No. 587 held on November 28, 2016 (Marga 13, 2073) has approved the "**Operational Risk Management Policy & Framework 2016**".

The Operational Risk Management Policy & Framework 2016 has been attached herewith for your necessary record, information and implementation.

Ramesh Raj Aryal
Chief Executive Officer

NCC Bank
नेपाल क्रेडिट एण्ड कमर्स बैंक लि.
Nepal Credit & Commerce Bank Ltd.

Operational Risk Management Policy

&

Framework

2016

(Approved by the Management Committee Meeting No.587)
(Meeting held on November 28, 2016)

November 2016

Table of Contents

Chapter – I: General

1) Background

Globalization of financial services, together with increased financial innovations, is making the activities of Financial Institutions and their risk profiles *(i.e. the level of risk across an institution's activities and/or risk categories)* more complex. Due to these developments, Operational Risk is becoming more pronounced. Operational Risk has garnered ample importance in risk management function of the Banks and Financial Institutions on the backdrop of rapid innovation within the financial products; technology deployed and increased complexity in the operations and functioning of the financial institutions. The pervasive nature of operational risks across all the functions make it imperative that a sound operational risk management framework that instills, monitors, reviews, and responses to pertinent operational risks issues is implemented at all functions, activities and levels of the bank.

All the applicable legal and regulatory frameworks and best practices applicable to the issue of Operational Risk Management have been duly taken care of, to the extent known, while drafting this Policy as an integral part of 'Risk Management Guidelines 2072 under Managing Operational Risk' of the bank. 'Operational Risk Management Policy 2016' shall come into force from the date of approval by the Board of Directors of Nepal Credit & Commerce Bank Limited.

The Board of Directors at any time by a notification, can suspend, cancel, add/delete or amend any of the provisions of this Policy.

It shall be the duty of all the concerned employees to make themselves acquainted with the rules/regulations/policies and procedures incorporated in this policy and other policies referred herein.

2) Definitions

Unless otherwise specifically indicated, the following terms used in Nepal Credit & Commerce Bank Operational Risk Management Policy, 2016 shall have the following meaning(s):

a) 'NCC Bank' or 'the Bank' means Nepal Credit & Commerce Bank Limited established under Bank and Financial Institution Act 2063 and Companies Act 2063 and under the Memorandum and Articles of Associations of the Bank.
b) 'Board/ Management Committee (Board)' or 'BOD' means Board of Directors of the Bank.
c) 'Board Level Committees/Sub Committees' means committees formed by the Board within the guidelines of Nepal Rastra Bank whose functions and authorities are as determined by the Board from time to time.
d) 'Risk Management Sub Committee' means committee formed under the chairmanship of the Chief Executive officer.
e) 'Corporate Governance Committee' means Committee formed by the Bank in order to monitor corporate governance status of the Bank on regular basis.
f) 'Chief Executive Officer (CEO)' means person appointed as Chief Executive Officer of the Bank.

g) 'Senior Management' means the Chief Executive Officer of the Bank and the Officials of the Bank delegated by the Chief Executive Officer who have direct accountability to the Chief Executive Officer.
h) 'Department Head' means the head of a particular Department/Unit of the Bank.
i) Branch Managers' means heads of branches of the Bank.
j) 'Employee' means a person engaged under full-time/part-time/contract employee in the Bank.
k) 'Transaction' means banking transactions as defined by the Banking and Financial Institutions Act and/or the Memorandum and Articles of Association of the Bank.
l) 'Memorandum and Articles of Associations' means Memorandum and Articles of Association of the Bank.
m) 'Risk Appetite' means the aggregate level and types of risk the Bank is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.
n) 'Risk Appetite Statement (RAS)' means the written articulation of the aggregate level and types of risk that the Bank will accept, or avoid, in order achieving its business objectives. It includes quantitative measures expressed relative to earnings, capital, risk measures, liquidity and other relevant measures as appropriate. It also includes qualitative statements to address reputation and conduct risks as well as money laundering and unethical practices.
o) 'Risk Appetite Framework (RAF)' means the overall approach, including policies, processes, controls and systems through which risk appetite is established, communicated and monitored. It includes a risk appetite statement, risk limits and an outline of the roles and responsibilities of those overseeing the implementation and monitoring of the RAF.
p) 'Risk Capacity' means the maximum amount of risk as bank is able to assume given its capital base, risk management and control measures, as well as its regulatory constraints.
q) 'Risk Limits' means specific quantitative measures or limits based on, for example, forward-looking assumptions that allocate the bank's aggregate Risk Appetite Statement to business lines, legal entities as relevant, specific risk categories, concentrations and, as appropriate, other measures.
r) 'Risk Management' means the processes established to ensure that all material risks and associated risk concentrations are identified, measured, limited, controlled, mitigated and reported on a timely and comprehensive basis.
s) 'Risk Profile' means Point in time assessment of the bank's gross (i.e. before the application of any mitigants) or, as appropriate, net risk exposures (i.e. after taking into account mitigants) aggregated within and across each relevant risk category based on current or forward looking assumptions.
t) "Duty of Care' means the duty of Board Members to decide and act on an informed and prudent basis with respect to the Bank.
u) 'Duty of Loyalty' means the duty of Board Members to act in good faith in the interest of the Bank. The duty of loyalty shall prevent individual Board members from acting in their own interest, or the interest of another individual or group, at the expense of the Bank and shareholders.
v) 'Control of Functions' means those functions that have a responsibility independent from management to provide objective assessment, reporting and/or assurance. This includes the risk management function, the compliance function, and the internal audit function.

w) 'Internal Control System' means a set of rules and controls governing the bank's organization and operational structure including reporting processes, and functions for risk management, compliance and internal audit.

Over then the terms specifically defined hereinabove, the terms used in various sections of this Policy shall have the same meaning as has been defined under various other policy documents of the Bank and the applicable laws of land, whenever relevant.

3) Meaning and Importance of Operational Risk Management

Basel Committee on Banking Supervision defines Operational Risk 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'. It further adds 'Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

Operational Risk is pervasive across all the functions of the Bank and is influenced by all resources, including human resources, systems and procedural designs, deployed by the Bank to carry out those functions. Operational risk can be caused by both internal and external sources such as fraud, business interruptions, system failures, damage to physical infrastructure, failure in execution and service delivery, inherent risks in products, customers, inadequacy in procedures or flawed process designs, and business practices. The risk can occur in any business function or the business supporting functions.

The effect of failure in any of the resource can have magnanimous repercussions across the Bank. This has convened higher scrutiny from the stakeholders of the Bank including the regulators. With due consideration to the importance of prudently managing the Operational Risk and to safeguard the Bank from any risks thus arising, a capital charge has been assigned specifically to buffer the effects of Operational Risk. Effective management of Operational Risk helps the bank to avoid unnecessary operational losses and helps the Bank to meet the Bank's strategic goals, as well as veneer the Bank from reputational depletion and adverse media.

4) Objectives of the Policy

The primary objectives behind formulation of this Policy are as under:

a) To lay down a framework for achieving robust operational risk management in alignment with regulatory requirements, best practice and the Bank's overall risk management policy;
b) To ensure that the Bank have adequate systems to identify, measure, monitor and control operational risk;
c) To ensure adequate, prioritized and focused attention from the board and senior management level on significant operational risk exposures and measures of mitigations; and
d) To ensure that a sound risk management culture is established throughout the bank.

5) Operational Risk Management Principles

Sound operational risk management is effective administering its portfolio of products, activities, processes, and systems.

The Basel Committee on Banking Supervision (Committee) articulated a framework of principles for the industry and supervisors in its Sound Practices for the Management and Supervision of Operational Risk (Sound Practices), published in February 2003. The sound practice and hence the knowledge and experience in the management of operational risk have continued to evolve. The practices on implementing operational risk management framework, loss data collection, impact analysis, governance, data collection and analysis, and modelling have emerged and are more refined.

The Committee updated the 2003 paper with Principles for the Sound Management of Operational Risk and the Role of Supervision 2011 to reflect the enhanced sound operational risk management practices in use by the industry. This document details eleven principles of sound operational risk management with its focus on (1) governance (2) risk management environment and (3) the role of disclosure.

The Guidelines – Principles for Sound Management of Operational Risk issued by Basel Committee on Banking Supervision and Nepal Rastra Bank, Risk Management Guidelines – 2010 have been collectively taken as the core basis for this policy.

6) Legislative and Regulatory Framework on Operational Risk Management

The following regulations currently in effect in Nepal have, directly or indirectly, addressed some provisions regarding Operational Risk Management of the Bank:

a) Unified Directives 1,5,6 issued by Nepal Rastra Bank
b) Risk Management Guidelines, 2010 issued by Nepal Rastra Bank
c) Information Technology Guidelines, 2012 issued by Nepal Rastra Bank

7) Nepal Credit & Commerce Bank's Policy on Operational Risk Management

The Bank is committed to be governed with a strong culture of risk management and ethical business practices and therefore to averse it from potentially damaging operational risk events and to be in a sound position to deal effectively with those events that do occur. The actions of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture.

The Bank is set to achieve clarity in expectations and accountabilities through well-defined delegation of authority to ensure that bank staffs understand their roles and responsibilities for risk, as well as their authority to act.

Similarly, the Bank shall use key control standards, key control self-assessments and key risk indicators as toolkits to identify, assess, monitor and control operational risk events through timely acknowledgement of emerging threats and underlying vulnerabilities.

The Bank shall also ensure highest level of governance standards and adherence to Code of Conduct and robust compliance to all regulatory as well as the Bank's internal policy, procedures and guidelines.

All the officials of the Bank shall not only be well-versed with all the policy documents of the Bank, applicable rules and regulations of the country, the directives/ circulars/ guidelines issued by various regulatory authorities but also comply with these policies, rules and regulations and directives/circulars/guidelines. If due to any reason whatsoever any deviation is required in the provisions contained in an internal policy document, a specific prior approval to this effect from the competent authorities shall be sought. However, waiver for deviating from the regulatory requirements shall not be provided.

Chapter II: Operational Risk Management Framework of the Bank

The Board envisages that by opting for sound Operational Risk Management practices, the bank will be able to gain respect, appreciation and confidence of all the stakeholders. These practices will also enhance image, goodwill and credibility of the Bank. It is also expected that the policy will play a vital role to mitigate operational risk which otherwise the Bank would be exposed to.

It is the strategy of the bank to indulge into activities the risks of which are fairly known and reasonable and in line with the risk appetite of the Bank.

Every product and services brought by the Bank are duly assessed with risks involved and mitigating measures are in built. It is mandatory that while executing day to day operations, compliance of the stipulated system, process and procedures are must.

It is the responsibility of all the concerned to manage identified, assessed, decided, implemented, operation risk function. Conscious efforts should be made to ensure that these policies are communicated at all levels and across entire value chain.

The Operational Risk Management Policy shall be reviewed periodically by Risk Management Sub Committee and the Risk Management Committee (RMC) at least once in a year and put forth to the board to ensure implementation and improvement of risk mitigation on a competitive level and also incorporate mitigations for emerging risks owing to internal and external factors. Depending upon the critically of internal operating environment and key external factors, review of the policy shall be holistic.

The Operational Risk Management Framework of the Bank typically consists of the following:

i) Board and Senior Management Oversight
ii) Operational Risk Function and Structure
iii) Framework for Risk Assessment and Quantification
iv) Framework for Risk Monitoring and Reporting
v) Enforcement of sound Operational Risk Management culture and practices
vi) Verification of Operational Risk Management Framework
vii) Control Functions
viii) Contingency Planning

8) Operational Risk Management Model

Operational Risk Management model occurs with the risk management framework as envisaged by the Corporate Governance Policy of the Bank with well-defined organizational responsibilities for risk management, typically referred as the three lines of defense:

i) The Business Units are the **first line of defense:**
The business units are responsible and accountable for the ongoing management of such risks. This includes identifying, assessing and reporting risk exposures and risk events. The Bank's risk culture shall be translated in the execution of

the responsibilities of the business unit. All the front office and client facing activity shall be included under the Business Unit.

ii) Risk Management Department headed by Chief Risk Officer, a compliance department and a legal department independent from the first line of defense shall act as the **second line of defense**; and

iii) An internal audit department independent from the first and second lines of defense shall act as **third line of defense.**

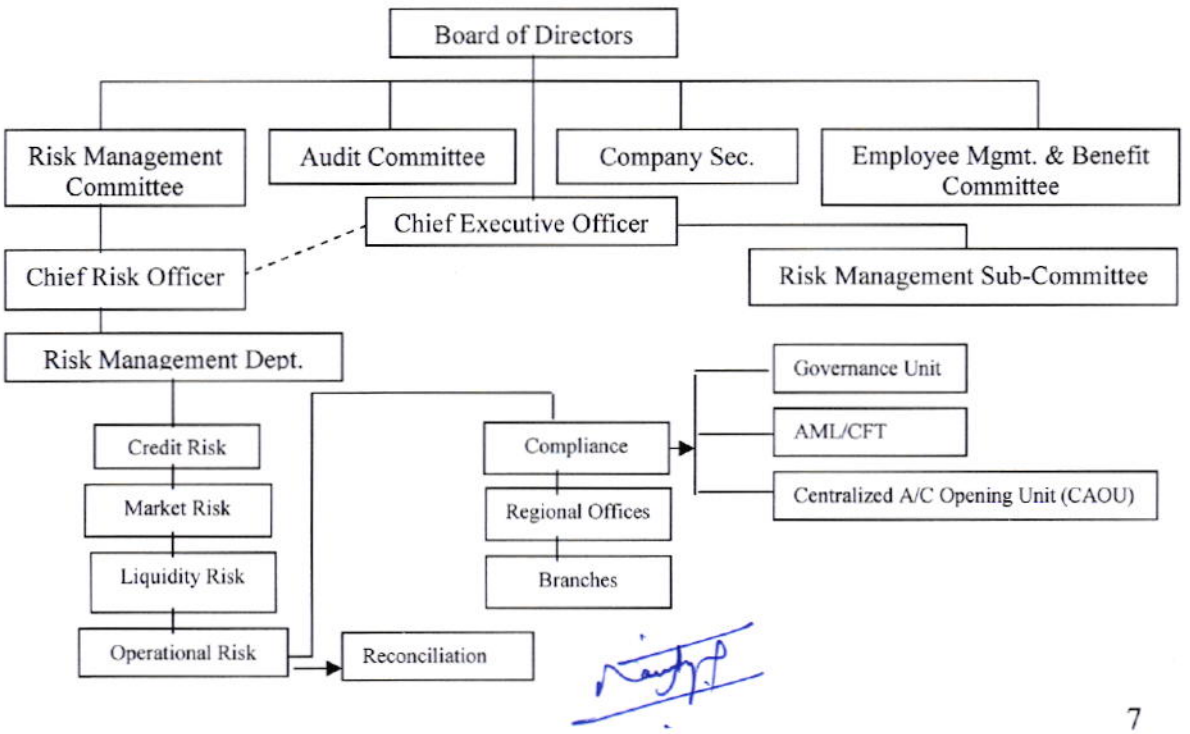
Risk Management Department headed by Chief Risk Officer in line with the Bank's Corporate Governance Policy, shall act as second line of defense in operational risk management of the Bank.

Key activities to be carried out by the Risk Management Department related to management of operational risk are as under:

- Identifying material individual, aggregate and emerging risks;
- Assessing these risks and measuring the bank's exposure to them;
- Supporting the board in its implementation, review and approval of the enterprise-wide operational risk framework which includes the bank's risk culture, risk appetite, Risk Appetite Statement and risk limits related to operational risks;
- Ongoing monitoring of the risk exposed activities and risk exposures to ensure they are in line with the approved risks appetite, and risk limits;
- Establishing an early warning or trigger system for breaches of the bank's risk appetite or limits;
- Influencing and, when necessary, challenging material risk decisions; and
- Reporting to senior management and the board or risk management committee, as appropriate, on all these items, including but not limited to proposing appropriate operational risk-mitigating actions.

9) Operational Risk Reporting Structure

The Bank shall have the following structure for reporting of Operational Risk issues in place for effective management of Operational Risks:



10)Operational Risk Management Processes

Following eight-step 'Operational Risk Management' (ORM) process will be adopted for managing operational risks at the Bank:

Step 1: Identification

The first step of managing new and unique operational risk is identification of such risk. It is especially challenging to define operational risk factors having a loss potential.

Step 2: Disclosure

Reporting shall be as prescribed and circulated from time to time in this regard.

Step 3: Grading Operational Risk (Prioritization and Classification)

This is a very critical step in establishing and effective operational Risk Monitoring system since this step determines, out of the large number of risk events, which ones will require and to what extent the attention of the limited resources of the financial institution. It is at this step a decision is made about the nature as well as the extent of the future attention (analysis, evaluation) that has to be given. Therefore, the grading process shall be well defined from the beginning and revised continuously to include lessons learned from an on-going stream of reports and analysis.

As a step in operational risk grading, the Policy requires qualitatively categorization potential incidents into a frequency – severity matrix, four such category has been identified for this purpose:

Risk Grading Table

High frequency – Low severity	High Frequency – High severity
Low frequency – Low Severity	Low Frequency – High Severity

Frequency ↑

Severity →

Category 1: High Frequency – high severity

These are the potential Operational Risk events chances of occurrence of which are high and the severity impact is also high. Risk Management Department will pay highest attention to such high frequency – high severity operational risk events.

Category 2: Low Frequency – high severity

Low frequency – high severity category include events having a major impact not only on the operations but also in terms of creating awareness of their existence.

Category 3: High Frequency – low severity

This category includes examples of operational loss events that occur frequently and cause relatively small losses and include transaction failure, credit card fraud, or accounting irregularities. The advantage of high frequency events is the possibility to create large databases on which statistical analysis can be accurately based upon. Appropriate statistical analysis would include estimation procedures, simulations, and regression analysis.

Category 4: Low Frequency – low severity

This category consists of operational risk events less likely to occur and the effect of which are less severe.

Step 4: Distribution

Once operational risk event information has been reported with appropriate categorization, it shall be directed to supervising authority at corporate level and to Risk Management Department (In case of Category 1 & 2) eventually. The supervising authority shall have re-classification authority as well. Thus it is mandatory for the Branch Operation In-Charge or designated official to report all such events to Risk Management Department.

Step 5: Analysis

The reported risk event shall be analyzed by Risk Management Department in coordination with expertise from related fields such as IT, Operations, legal etc. The casual effect relationship of the event shall be identified; actions plan shall be developed and implemented with adequate mitigation measures.

Step 6: Solution Identification

Once causes of a problem are identified, the next step is finding viable solutions for each cause. Few important points for this step are:

- Matching solutions to causes, hence ensuring that each cause has been addressed
- Reviewing identified solutions to ensure that they shall not be the cause of other risk events themselves (management of change)
- If possible, include a member of the department responsible for implementation of the solution in the discussion.

Step 7: Dissemination

Once an action (or a set of actions) is determined:

- The action shall be approved by the proper channels and assigned to the concerned department/Branch or at country level to implement.

- A larger group including other departments may need to be informed of the incident and the actions taken

Both of these activities are highly dependent on the nature of the operational risk issues taken into consideration and must be completed to ensure systems effectiveness.

Step 8: Execution and Closure

This is the step where all actions are completed including follow-up with the concerned departments and personnel. It is at this step that one needs to identify and track all open actions and pursue with the person responsible for their closure. These activities may involve seeking approval from higher management to obtain priority for implementation procedures.

Any new and unique operational risks events might subsequently need regular monitoring by including in 'Operational risk monitoring and Reporting Framework (ORMRF)'. The reporting format, frequency and responsibility shall be as defined by RMD.

11) Appetite and Measurement of Operational Risk

The major purpose of an Operational risk appetite statement is to provide lucidity on the quantity and type of operational risks that the Bank is willing to accept as well as a better understanding of the trade-offs between risk and returns. The process of defined risk appetite and monitoring adherence to it can help drive more informed decisions about capital allocation and ensure that strategic business decisions are made with a complete understanding of the risks and the capacity to manage those risks.

Risk Appetite of the Bank

The overall operational risk appetite and tolerance statement shall encapsulate the changes in environmental factors, bank's financial condition, quality of control standards and control environment, loss data, changes in volume of business and activity, and occurrence of operational risk events. The operational risk appetite and tolerance statement shall be revised by the approval of the Risk Management Committee as and when required, but at least once in a year.

The risk appetite shall not exceed 25% of the average of sum of percentage of Risk Weighted Exposure for Operational Risk of past three years, calculated as:

=[{(RWEop.n/RWE.n)*100%}+{(RWEop.n/RWE.n)*100%}+{(RWEop.n/RWE.n)*100%}]

Where, RWEop.n is Risk Weighted Exposure for Operational Risk for year n

RWE.n is Total Risk Weighted Exposure for Operational Risk for year n

n= year 1, year 2 and year 3

Measurement and Quantification of Operational Risk

The measurement and quantification shall be carried out through:

1. Operational Risk Loss Data Base and Near Misses
2. Modified Internal Measurement Approach

11.1 Operational Risk Loss Data Base and Near Misses:

Operational Risk and Loss Reports from the basis for Operational Risk Management at the Bank as it allows the bank to have a robust risk mitigation, control and monitoring process, decision making based on analysis of Operational Risk and Loss Data.

The Risk Management Department shall maintain database of Operational Risk event. The database shall be maintained for:

1. Operational Risk Events
2. Near Miss Events

11.1.1 Classification of Operational Risk Event Type

Such database shall be based on operational risk event type. The classifications of Loss Event type are:

1. **Internal Fraud:** Internal fraud events include acts, involving at least one internal party, with the intention to defraud, misappropriate property or circumvent regulations, the law or the Bank's policy. The internal fraud also includes occupational fraud in which am employee misuses the Bank's resources for personal gains.
2. **External Fraud:** External fraud events include acts by a third party with the intention to defraud, misappropriate property or circumvent the law with against the good standing of the Bank.
3. **Employment Practices and Workplace Safety:** The risk events arising from acts inconsistent with employment, health or safety laws or arrangements, from payment of personal injury claims, or from discrimination events etc. are captured as employment Practices and workplace safety. Occupational hazards are also included.
4. **Clients, Products & Business Practices:** The risk events such as fiduciary breaches, misuse of confidential information, market manipulation, insider trading, **money laundering** etc. are captured under clients, products and business practices. This risk arises due to unintentional or negligent failure to meet professional obligations and or due to flawed design of products.
5. **Damage to Physical Assets:** The risk events arising due to natural catastrophe, act of terrorism, negligent handlings of assets by employee etc. are captured under Damage to Physical Assets event type.
6. **Business Disruption and system failure:** The risk events arising from failures in hardware, software, network, outage in utilities etc. are captured under Business Disruption and system failure.

The detailed Loss Event Type Classification has been attached to this policy as ***Annexure -1.***

11.1.2 Reporting of Operational Risk Events

As the risk events causing or with latency to cause operational loss is pervasive across all functions, it is the primary duty and responsibility of the units/branches/departments to report the risk events to the Risk Management Department.

11.1.3 Access to Operational Risk Event Data Repository:

The access to the data repository shall be provided only to the assigned staff member of Risk Management Department. Access to any other party requesting the access to the repository shall require the approval of Chief Risk Officer or Chief Executive Officer.

11.1.4 Quantification of Operational Risk Events:

The quantification of the risk events shall be as follows:

11.1.4.1 Operational Risk Loss Event:

The loss borne due to operational risk event shall be reported and recorded in the face value of the financial loss.

11.1.4.2 Operational Risk Gain Event:

The operational risk events that generate a gain, such gain shall be reported and recorded in the face value of the financial gain.

11.1.4.3 Operational Risk Events where no financial loss occurred:

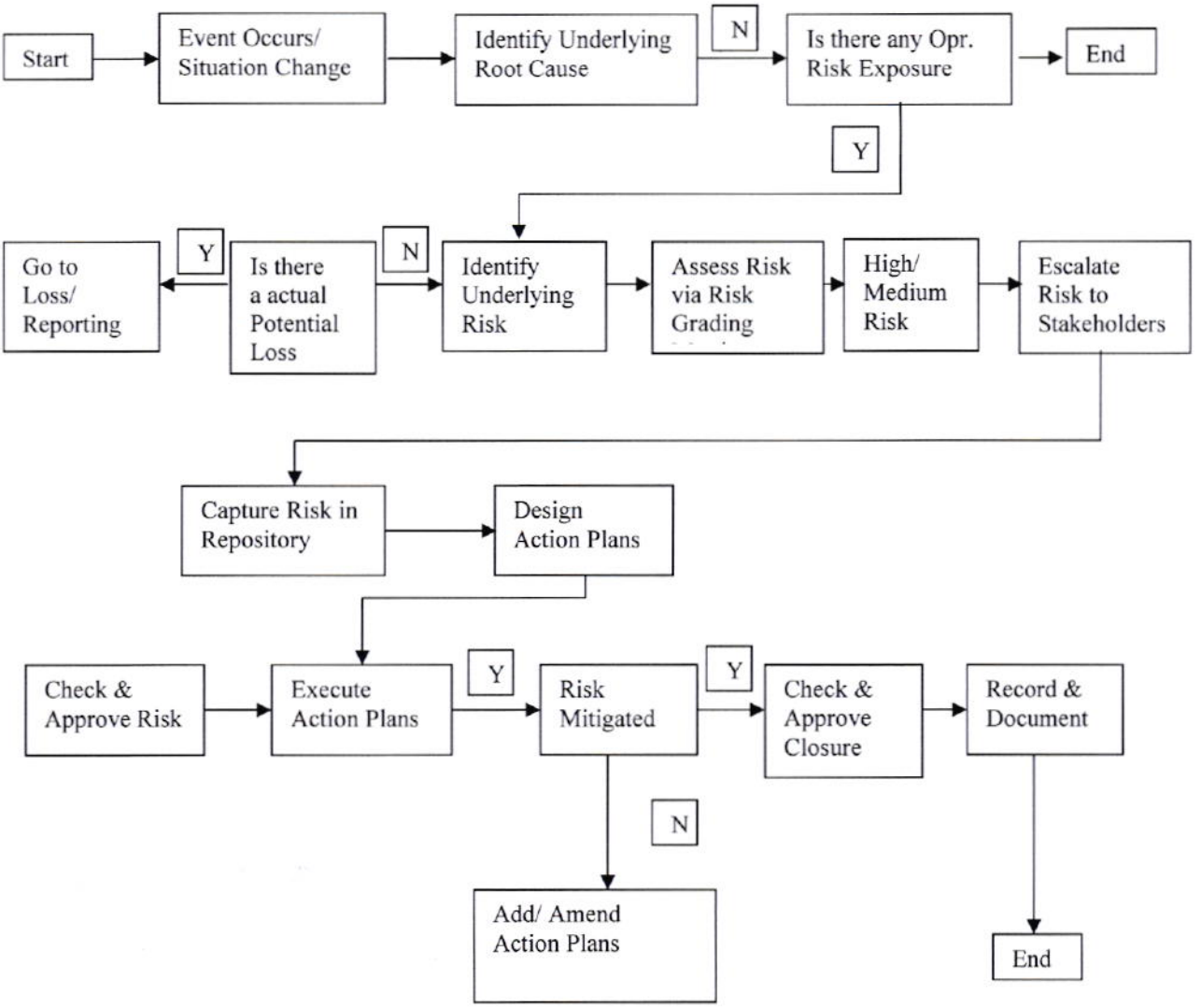
The operational loss shall be calculated based of counterfactual assumption and the latency of loss that could have occurred due to the event.

11.1.4.4 Near Miss Events:

The operational loss shall be calculated based of Near Miss Events assumptions and the latency of loss that could have occurred due to the event.

11.1.4.5 Risk Reporting and Recording Process:

The risk reporting and loss recording process has been outlined in the following flow diagram:



11.2 Modified Internal Measurement Approach

The Bank shall use the granularity concept to identify to the extent possible the quantifiable operational risk exposure within each business line and the activities carried out therein.

A risk factor shall be assigned to each business function based on the possibility of occurrence and severity to calculate the risk exposure. This calculation shall be for the purpose of analysis and monitoring of operational risk inherent in the activities carried under different business lines, and the distribution of risk across business functions of the Bank.

Based on the risk event reported and the loss incurred, the activity and the function in which the loss occurred shall be assigned an operational risk loss weight age as the percentage of the actual loss incurred to the Bank's Risk Weighted Exposure for Operational Risk.

11.3 Monitoring of Measured Risk against Risk Appetite:

The total Operational Risk of the Bank calculated under this policy shall be compared against the operational risk appetite of the Bank. Where the calculated risk exceeds the risk appetite of the Bank, the Risk Management Department shall review the risk management process, identify the cause and activities leading to the overshoot, report to Risk Management Committee and the Board, design action plan and implement the action plan approved by Board on the recommendation of Risk Management Committee. The Risk Management Sub Committee also discuss and review the risk the risk management process, identify the cause and activities leading to the overshoot, report to Risk Management Committee and the Board.

12)Risk Management Tool Kits

The bank shall use the following tool kits for the effective management of Operational Risk Management. These toolkits serve as the fundamentals for identification, assessment, and management of operational risk and shall be embedded in the operational risk management framework of the Bank. These toolkits shall be deployed proactively in an anticipatory fashion to recognize and manage risk in a forward looking manner:

1. Key Control Standards
2. Key Control Self Assessment
3. Key Risk Indicators

12.1 Key Control Standards:

Key control standards are bare minimum qualitative control standards to be attained by all the functions. The control standards are segregated as:

S.N.	Standard	Control Scope
1	Organization	Clear segregation of roles and responsibilities Updated Delegation of Authority in commensurate with the Bank's Policies Duly recorded handover, takeover procedures during staff movements/ resignation etc.
2	Compliance	Compliance with all Laws of the land Compliance with all regulatory requirements including reporting Impact of regulatory changes Compliance with Employees Code of Conduct Maintenance of Customer Confidentiality
3	Human Resource	Competencies in assigned roles and responsibilities

		Mandatory leaves and peer reviews Adequate staffing Work Environment and workplace hazards Adequacy in staff members records and Know Your Employee
4	Product	Adequate risk mitigation in product support processes Products in alignment with regulatory compliance and defined risk appetite
5	Contingency Protection	Business Continuity Plan Disaster Recovery Plan Operation during Disaster
6	Security and Protection	Adequacy in security arrangements and alarm system Adequacy in protection measures for physical assets Adequacy in protection of Information Adequacy in protection of intellectual property of the Bank Adequacy in protection measures against cyber threats Adequacy in staff members security and control of work place hazards
7	Reputation	Service Delivery Customer Complaints External Environmental threats to reputation
8	Audit	Audit Plan Adequacy of Audit Issues raised by Audit
9	Risk Assessment	Adequate assessment of Operational risk by Units/ Departments/ Branches Adherence to Operational Risk Management Policies and Guidelines Key Control Self-Assessment
10	Finance	Adherence to prescribed Accounting Standards Assets/ liabilities reconciliation

		General Ledger reviews and accuracy

The Risk Management Department shall roll out Key Control Standards to all the Units/ Departments/ Branches along with the control and primarily responsible authority. The KCS shall be revised on an annual basis by RMD. Such revision shall take into account the output of Key Control Self-Assessment (KCSA), issues raised by Audit, risk reporting, and risk assessment carried out by Risk Management Department.

12.2 Key Control Self-Assessment (KCSA)

Key Control Self-Assessment is checks used by functional supervisors to ensure that the controls designed for mitigation of Operational Risk are duly adhered to. The other outcome of KCSA are whether the controls are adequate in the given operating environment, identification of internal and external issues that may result in Operational Risk events, and whether the given controls are effective.

The Risk Management Department shall facilitate carrying out of KCSA on a periodic frequency according to the nature of control standard and risk indicator. The Operational Risk reporting shall also include components of KCSA.

12.3 Key Risk Indicators (KRIs):

The major objective of Key Risk Indicators (KRIs) is to enable the Bank to identify current risk exposure and emerging risk trends, highlight control weaknesses and allow for the strengthening of poor controls and facilitate the risk reporting and escalation process.

The Bank shall deploy both the leading and lagging Key Risk Indicators to the extent possible to effectively manage existing and anticipated risk events.

The Risk Management Department shall on a periodic basis or as and when required but at least once a year, update the Key Risk Indicators based on the Control Standards and Risk Assessment. The Key Risk Indicators shall be monitored within assigned frequency and shall be an integral part of the risk reporting of the Bank. Some of the indicators are presented as ***Annexure-2*** to this document.

13) Verification of Operational Risk Management Framework

Verification activities test the effectiveness of the overall Framework, consistent with policies approved by the board of directors, and also test validation processes to ensure they are implemented in a manner consistent with established bank policies.

The internal and/or external qualified independent parties shall carry out verification of the Bank's Operational Risk Management Framework on a periodic basis at least once during a fiscal year. Such verification may be carried out by the Bank's internal Audit as well.

14) Periodic Review of Effectiveness of Operational Risk Management Framework

The Operational Risk Management system and framework implemented by the Bank shall be reviewed at least once a year and if any new Policy/Manual/Standard Operating Procedure/Guideline is deemed desirable, these shall be formulated as soon as possible. Risk Management Department of the Bank shall be responsible for this.

The competent authority for revision of a document shall be the authority which initially approved the document.

15) Enforcement and Effective Discharge of Roles & Responsibilities

The roles and responsibilities for achieving an effective and robust management of the Operational Risk of the Bank shall be as articulated below:

15.1 Board of Directors

The board of directors should take the lead in establishing a strong risk management culture. The board of directors, risk management committee and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organization. The Board has overall responsibility for the Bank; including approving and overseeing the implementation of the Bank's risk strategy and corporate governance. The Board also provides effective oversight of the Operational Risk Management function and framework.

15.2 Risk Management Committee

The Risk Management Committee should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. The Risk Management Committee also provides effective oversight of the Operational Risk Management function and framework.

15.3 Risk Management Sub Committee

The Risk Management Sub Committee shall put in place the operational risk management framework established by the board of directors and risk management committee. The Committee shall ensure that bank activities are conducted professionally and monitor the risks. The committee shall check, review and ensure that the necessary resources are available to manage operational risk activity. The Committee meets at least every month and reviews the adequacy and effectiveness of risk management process also measure and monitors risk at operational level including financial crime compliance risk.

15.4 Senior Management

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. The Bank management is required to understand and therefore translate into execution with proper mitigation measures the nature and complexity of the risks inherent in the portfolio of bank products, services and activities. This is particularly important for operational risk, given that operational risk is inherent in all business products, activities, processes and systems. The senior management shall ensure the components of the framework is fully integrated into the overall risk management processes of the bank at all level, functions and process.

a. Roles and Responsibilities of the Chief Executive Officer

It shall be the responsibility of the CEO to ensure that the Bank has a strong control environment and that the policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies systems are utilized in the management of operational risk of the Bank.

b. Role of Department Heads/Branch Managers

The department heads/ branch managers shall ensure that the standards set for identification, assessment, monitoring and control of the overall operational risk as well a risk specific to their line of function is duly complied with without any deviation. It shall also be the ultimate responsibility of the department heads/ branch managers that operational risk events are timely reported.

15.5 All Employees (including the Senior Management)

All the employees of the Bank shall keep themselves fully aware and updated (at least) of the Bylaws/ Policies/ Manuals/ Guidelines/ Product Papers/ Procedural Documents/Standard Operating Procedures/ Circulars as well as the legal and regulatory requirements in so far as they are applicable to their respective areas of work. Employees at supervisory role must ensure that employees under their supervision are fully aware/ updated of the applicable internal as well as external requirements.

Chapter-III: Miscellaneous

16) Interpretation, Amendment and Review

The Board of Directors of the Bank shall be the final authority to interpret various provisions contained in this Policy and to approve amendments or review, as necessary, from time to time to such provisions.

If any provision contained in this Policy contradicts against any laws of land, regulatory pronouncements, or requirement of any internal policy document enforced/amended subsequent to the approval or revision of this policy, the provisions contained in this policy shall be deemed to have accordingly amended to the extent of contradiction.

This policy shall be reviewed on an annual basis for the purpose of updating it in line with legal and regulatory changes and in order to achieve a robust and effective Operational Risk Management framework across all levels and activities of the Bank.

17) Repeal and Saving

Any acts done and actions taken before the formulation and revision of this policy shall be deemed to have been carried out in due compliance with this Policy.

18) Annexure

The following Annexure shall construe an integral component of this Policy.

Annexure 1: **Detailed Loss Event Classification Type**

Annexure 2: **Data Collection for Monitoring of Controls and Risk Indicators (Examples)**

Annexure 1

Detailed Loss Event Classification Type

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (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.	Unauthorized Activity	Transactions not reported (intentional) Trans type unauthorized (w/monetary loss), Mis-marking 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 take-over/ impersonation/ etc. Tax non-compliance/ evasion (willful) Bribes/ kickbacks Insider trading (not on firm'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 (w/ monetary loss)
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/ discrimination events	Employee Relations	Compensation, benefit, termination issues Organized labor activity
		Safe Environment	General liability (slip and fall, etc,) Employees health & safety rules events Workers compensation
		Diversity & Discrimination	All discrimination types
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches/ guideline violations Suitability/ 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 (on firm's account) Unlicensed activity Money laundering
		Product Flaws	Product defects (unauthorized etc.) Model errors

		Selection, Sponsorship & Exposure	Failure to investigate client 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 disaster 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 outage/ disruptions
Execution, Delivery & Process Management	Losses from failed transaction 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 Delivery failure Collateral management failure

		Monitoring and Reporting	Reference Data Maintenance. Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions/ disclaimers missing Legal documents missing/ incomplete
		Customer/ Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty ms performance Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing Vendor disputes

Annexure 2

Data Collection for Monitoring of Controls and Risk Indicators (Examples)

S. No.	Data Collection Indicators	Monitoring Frequency	Trigger Level	Mitigation Measure	Ownership of Action Plan	Escalation
	General Banking					
1	Output Checking					
2	Account Opened with Pending Documents					
3	Cheque Requested but not delivery					
4	ATM card request but not received					
5	ATM Card Received but delivered					
6	Cash Short Report					
7	Cash Excess Report					
	Clearing					
8	Cash and Cash Value Found in Branch Premises					
9	Exhibit of cheque return inward					
10	Exhibit of cheque return outward					
	Reconciliation					
11	Inter Department Account					
12	ATM Reconciliation					
13	Dividend Reconciliation					
14	Suspense Account Reconciliation					
15	Fixed Assets Reconciliation					
16	NOSTRO Reconciliation					
	Account					
17	Exhibit of Account Payable					
18	Exhibit of Account Receivable					
19	Exhibit of Payable Account others					
20	MC not presented					

21	Exhibit of DD not presented more than 3 months					
22	Exhibit of Stale DD					
23	Exhibit of Dormant Account					
	Dormant Account					
24	Exhibit of Blocked/ freeze Accounts					
25	Exhibit of Blocked/ freeze Accounts activated					
26	Server down time					
27	ATM down time					
	Abnormal Event Reporting					
28	Crucial Machine Break Down					
	Security Report					
29	Branch security Highlight					
30	Abnormal Security Event during the month					
31	Business Disaster Reporting					
32	System Disaster Report					
33	Report on issues relating to Handling Vault Key and Password					
	Insurance Policy near Expiry					
34	If any Policy (Vehicle, Assets)					
35	Insurance Claim Made					
36	Insurance Claim Receivable					
37	Fire Extinguisher near Expiry					
	Deadline Report					
38	Renewal Due (FX licensing, Blue Book, pollution Test, Metropolitan Tax)					
	Fixed Assets Report					
39	Assets Purchase, Transfer and sales report					
40	Fixed Assets Damage Report					
41	Work Place safety report					
	Guarantee and LC Issued					
42	List of LC Expired					

43	List of Guarantee Expired					
44	List of contingencies not reversed					
45	List of FD matured					
46	List of Claim in Issued Guarantee					
47	List of Claim on issued Good for Payment cheque					
	Others					
48	Remittance Awaiting Disposal					
49	Details of Term Deposit interest pending					
50	Details of Matured Term Deposit					
51	Review of Guard Register					
52	Review of Attendance					
53	Petty Cash Reconciliation					
54	Fixed Assets and Depreciation Reconciliation					
55	Stock Stationery Reconciliation					
56	Record Management Review					
57	Statue of KYC customer					
58	Handling Vault key (ATM and vault key)					
59	Error Reporting					
60	CCTV reporting (90 Days)					
61	Checking of Teller Alarms/ fire Alarm					
62	Security Alertness Check					
63	Exhibit of Bills Documents Purchase					
64	Exhibit of outward collection items					
65	Physical check of Cash in Vault					
66	Physical check of Cash items					
67	Cash Value documents Reconciliation					
68	Key custodian report					
69	Details of other Assets					
70	Service Log of Assets					

71	Details of Total Liability					
72	Fuel consumption Details					
73	Vehicle log book					
74	Logistic Support					
75	Staff Leave Management					
76	INR ATM Cards Details					
77	ATM Card Block List					
78	INR Transaction					
79	Suspicious Transaction reporting					
80	Legal Cases Status					
81	Cash in Transit					