

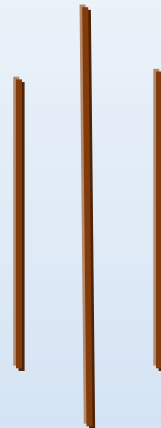


# **NCC Bank**

**नेपाल क्रेडिट एण्ड कर्मास बैंक लि.  
Nepal Credit & Commerce Bank Ltd.**

*Your Business Bank*

## **Operation Risk Management Policy & Framework 2018**



**Nepal Credit And Commerce Bank Ltd  
Bagbazar, Kathmandu**

**Approved by:**  
706<sup>th</sup> Board Meeting  
Held on 2075-05-20 (5<sup>th</sup> September, 2018)

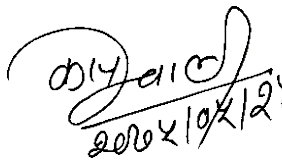


# **NCC Bank**

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

*Your Business Bank*

The Board Meeting No. 706<sup>th</sup>  
held on 2075.05.20 (5<sup>th</sup> September, 2018)  
has decided to approved, the  
**"Operation Risk Management Policy & Framework  
2018"**

  
2075/05/20



**Kapil Gnawali**  
Company secretary

### **Version History**

<b>Version History</b>	<b>Name of Document</b>	<b>Approving Authority</b>	<b>Date of Approval</b>
1 <sup>st</sup>	Operation Risk Management Policy and Framework, 2016	Management Committee	November 28, 2016
2 <sup>nd</sup>	Operation Risk Management Policy & Framework, 2018	Board of Director	

## **Approval Sheet**

<b>Particulars</b>	<b>Name and Designation</b>	<b>Signature</b>	<b>Date</b>
Prepared By	Saroj Bhandari Operation, Market and Liquidity Risk Management Department		
Reviewed and Supported By	Mukunda Subedi Chief Risk Officer		
Supported for Board Approval	Ramesh Raj Aryal Chief Executive Officer		
<b><u>Board of Directors</u></b>			

## **Table of Contents**

<b>1. Introduction.....</b>	<b>0</b>
<b>2. Objectives.....</b>	<b>1</b>
<b>3. Operation Risk Management Structure .....</b>	<b>1</b>
<b>4. Roles and Responsibilities .....</b>	<b>2</b>
4.1 Board of Directors.....	2
4.2 Risk Management Committee.....	2
4.3 CEO and Senior Level Management .....	2
4.4 Risk Management Sub Committee .....	2
4.5 Chief Risk Officer (CRO).....	2
4.6 Operational Risk Management Department (ORMD).....	3
4.7 Executives / Departments / Branches .....	3
<b>5. Risk Management Process .....</b>	<b>3</b>
5.1 Risk Identification and Assessment .....	3
5.2 Risk Measurement .....	4
5.3 Risk Monitoring .....	8
5.4 Risk Control and Mitigation .....	8
<b>6. Capital Measurement and Operational Loss Limit.....</b>	<b>9</b>
6.1 Capital Measurement .....	9
6.2 Operational Loss Limits.....	9
<b>7. Risk Treatment Strategies.....</b>	<b>9</b>
7.1 Avoidance: .....	10
7.2 Reduce: .....	10
7.3 Share / Transfer:.....	10
7.4 Acceptance: .....	10
<b>8. Operational Risk Management Model.....</b>	<b>10</b>
<b>9. Risk Management Tools .....</b>	<b>11</b>
9.1 Key Control Standards .....	11
9.2 Business / Functional Line Mapping .....	11
9.3 Key Risk Indicators (KRIs) / Early Warning Signals (EWS).....	12
9.4 Contingency Planning.....	12
9.5 Staff Training and Development Program .....	12

9.6 Revenue Leakage Monitoring.....	13
9.7 Turnaround Time .....	13
<b>10. Basic Operational Risk Measures.....</b>	<b>13</b>
10.1 General Banking .....	13
10.2 Information Technology System.....	1
10.3 Credit Administration Functions.....	2
10.4 Human Resource Management Function .....	3
10.5 General Administration Functions .....	4
10.6 Compliance Functions .....	5
<b>11. Disclosure Requirements.....</b>	<b>5</b>
<b>12. Implementation, Review and Updates .....</b>	<b>5</b>
<b>Annexure-1: Key Control Standards .....</b>	<b>6</b>
<b>Annexure-2: Key Risk Indicators (KRIs) / Early Warning Signals (EWS) .....</b>	<b>10</b>

# Operation Risk Management Policy & Framework, 2018

## 1. Introduction

Operational risk is the "risk of loss resulting from inadequate internal processes, people, and systems or from external events". Increased complexity and sophistication of operations, increased volume of transactions, innovation in new technology, emergence of E-commerce, acquisition & merger, globalization of financial services making the Bank's activities more complex and risk profile.

Operational risk management encompasses the mechanisms, tools, policies, procedures and process including management oversight, to identify, assess, monitor, report and control operational risk.

Bank classifies the operations risk event as follows:

- **Internal Fraud:** includes acts, involving at least one internal party, with the intention to defraud, misappropriate property or circumvent regulations, law or Bank's policy. For example: intentional misreporting of positions, employee theft, insider trading etc.
- **External Fraud:** includes acts by a third party with the intention to defraud, misappropriate property or circumvent the law against the good standing of the bank. For example, robbery, forgery, cheque kiting, hacking etc.
- **Employment Practices and Workplace Safety:** includes acts inconsistent with employment, health or safety or occupational hazards. For example, workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, general liability etc.
- **Customer, Products and Business Practices:** Fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, market manipulation, insider trading, money laundering and sale of unauthorized products.
- **Damage to Physical Assets:** Terrorism, vandalism, earthquakes, negligent handlings of assets by employee, fires and floods.
- **Business Disruption and System Failures:** Hardware and software failures, network problem, telecommunication problems and utility outages.
- **Execution, Delivery and Process Management:** Data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty and vendor disputes.

This Policy Framework has been prepared in line with the Risk Management Guidelines of the Bank and the regulatory requirement. The document has outlined the Banks initiative towards management of operational risk so that objective of the bank can be achieved optimally. It shall be the duty of all the staff members of the Bank to make themselves acquainted with the provisions incorporated in this policy and other policies referred herein.

*Signature*  
2024/02/28



## 2. Objectives

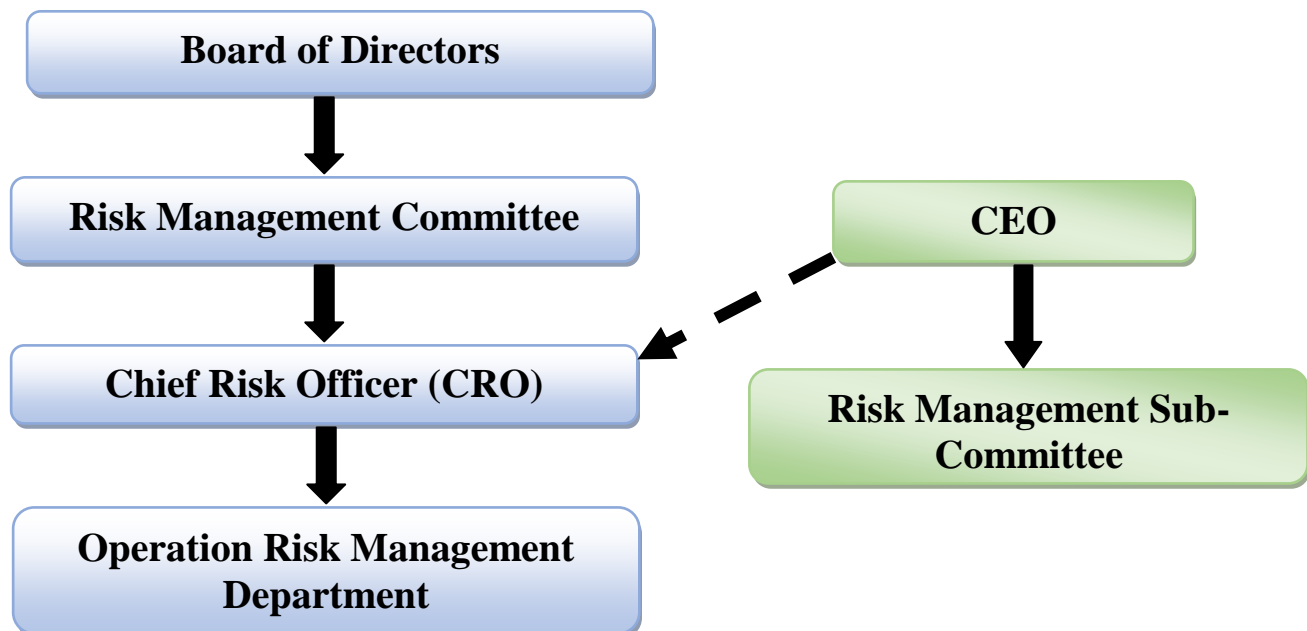
This policy has been formulated for guiding the bank to identify, access, measure, monitor, control and mitigate the operation risk. Followings are the objectives behind formulation of this policy:

- 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;
- To ensure that the Bank have adequate systems to identify, measure, monitor and control operation risk;
- To ensure adequate, prioritized and focused attention from the board and senior management level on significant operational risk exposures and measures of mitigations; and
- To ensure that a sound risk management culture is established throughout the bank

## 3. Operation Risk Management Structure

Bank shall have a separate department to look the issues and monitoring the operation risk. The department put continuous efforts and vision for the identification, assessment, measuring, monitoring and controlling the operations issues or losses. It collects the issues from concerned business line and uses it for the overall development of operation risk management practice in the bank. The department will report to the Chief Risk Officer and shall present the operational risk issue in Risk Management Sub-Committee and Board level Risk Management Committee.

The operational risk management structure of the Bank shall be as follows:



Every staff of the bank shall takes the responsibility of controlling risk or losses while performing their duties. Bank integrate it systems and procedures as a primary risk culture and risk mitigations.

*Signature*  
2020/10/28





#### **4. Roles and Responsibilities**

Roles and responsibilities of all concerned shall be to understand for identifying, assessing, monitoring, measuring and controlling operation risks. Bank shall assigned the following responsibilities, but not limited, to following functions:

##### **4.1 Board of Directors**

Board of Directors shall be primarily responsible for ensuring in place an effective operational risk management culture at the Bank. Board of Directors is also responsible to approve appropriate operational risk management policy, strategy and overseeing the implementation status. Board of Director shall review the operational risk associated with new products, activities or system before put into implementation on policy and strategy level.

##### **4.2 Risk Management Committee**

Risk management committee shall be responsible for review the operational risk profile of the bank, understand the future challenges and threats and concur on areas of highest priority and related mitigation strategy. Committee shall review the operational risk appetite, adequacy of resources being assigned to mitigate risks, reinforce culture and awareness of operational management throughout the bank and recommend suitable control/mitigating strategy for management of operational risk. The committee periodically updates the status of risks to the Board.

##### **4.3 CEO and Senior Level Management**

CEO and senior level management is primarily responsible for implementing the operational risk management policy and strategy approved by board and formulate appropriate procedures, guidelines, framework for the management of operational risk. CEO and Senior Management shall ensure that Bank has a strong control environment, formulated policies, process, system, internal control, risk mitigating strategy are in effective implementations and the staff members of the bank are well versed with banks operational risk management strategy.


##### **4.4 Risk Management Sub Committee**

Risk Management Sub Committee shall ensure the implementation of the operational risk management policy and framework. The committee shall ensure the 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. Committee also ensure the adequacy and effectiveness of risk management process in the Bank.

##### **4.5 Chief Risk Officer (CRO)**

Chief Risk Officer (CRO) shall be responsible for overall monitoring of the operational risk activities of the Bank. CRO shall support the CEO, Risk Management Committee and Board for implementation, review and approval of risk governance framework of the Bank. CRO shall ensure the establishment of early warning or trigger system for breaches of the bank's risk appetite or limits. CRO shall ensure the operational risk-taking activities and operational risk exposures are in line with the board-approved risk appetite, risk limit and capital planning. CRO shall report to the

*Handwritten signature and date:*  
2020/10/28



Risk Management Committee and updates to CEO on operational risk profile of the bank and all operational risk-mitigating activities of the Bank.

#### **4.6 Operational Risk Management Department (ORMD)**

Primary responsibility of the Operational Risk Management Department is to disseminate and implement the operational risk management policies, strategy, procedures, guidelines and framework in the bank. ORMD shall report all issues and status of the operational risk profile of the bank to the CRO and Risk Management Sub-Committee (RMSC). ORMD shall identify, access, measure, monitor and report the operational risk. Quantitative measurement of operational risk level of the branches and overall bank, review and report and feedback of the operational risk incident, monitoring of material exposures to losses, detecting and providing recommendation for the correction of deficiencies in the related policies, procedures and process shall be the responsibility of ORMD. ORMD shall develop the Key Risk Indicators (KRI), Early Warning Signals (EWS), and Risk and Control Self-Assessment (RCSA) etc.

#### **4.7 Executives / Departments / Branches**

Executives / Departments and Branches are responsible to ensure the implementation of risk parameters and principles as per the product, policies and procedures. Executives / Departments and Branches shall report the issues and incidents to the risk management department. Executives / Departments and Branches shall maintain zero level of non-compliance and ensure the prudent / ethical banking on the day to day functionality maintaining the well practice of risk culture and risk understanding.

### **5. Risk Management Process**


#### **5.1 Risk Identification and Assessment**

Risk identification is paramount for the subsequent development of a possible operational risk monitoring and control system. Effective risk identification considers both internal factors (such as: the bank's structure, the nature of activities, quality of human resources, organizational changes and employee turnover) and external factors (such as: changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives. Operational risk can be arose in the bank mainly from following weakness:

- Inadequate recognition and assessment of the risk of banking activities
- Lack of control culture
- Absence / failure of key control structures
- Inadequate communication
- Inadequate / ineffective audit and compliance programs
- Aggressiveness on sales compromising risk mitigation
- Inadequate staff competency

Bank shall use the various tools for identification and assessment of the operational risk. Common tools that can be used on identifying and assessing operational risk are the workshop, interactions, score card, risk mapping, risk indicators etc. Operational risk associated with all material products, activities, processes and systems shall be listed out for the identification and assessment.

*Handwritten signature and date:*  
2024/10/28



Following tools shall be adopted to assess the vulnerabilities of identified risks.

- **Risk and Control Self-Assessment (RCSA):** RCSA is a process through which operational risks and the effectiveness of controls are assessed and examined. The objective is to provide reasonable assurance that all business objectives will be met. The RCSA entities shall be identified, which shall be subject to an annual independent review by internal auditor.
- **Business Process Mapping with Risk Type:** Business process mappings identify the key steps in business processes, activities and organizational functions and the associated risk points. It reveals individual risks, risk interdependencies and areas of control or risk management weakness and helps to prioritize subsequent management action.
- **Key Risk Indicators (KRI) / Key Performance Indicators (KPI) / Early Warning Signals (EWS):** KRI and KPI are risk metrics and/or statistics that provide insight into a bank's risk exposure which are used to monitor the main drivers of exposure associated with key risks. This also provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures and potential loss. Bank shall use these indicators to access the operational risk on monthly basis.
- **Scenario Analysis:** Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Bank shall use scenario analysis as and when needed.
- **Audit Findings & Compliance Reviews:** Findings observed by audit (internal, statutory, NRB or special audit) and compliance review can provide insights into the bank's risk position that shall be used by the Bank as indicator of operational risk. Internal audit report shall separately disclosed the operation risk on the audit of branches and departments.

## 5.2 Risk Measurement

Risk Management process include risk measurement of the identified risk associated with material products, activities, processes and systems. Bank shall follow the steps outlined below for measuring operational risk.

- Based up on past experiences and audit reports, capture all the loss events data.
- Actual losses are captured and relates to the loss events data.
- Actual loss data is compared to the captured loss events data based on frequency and severity of events. By frequency mean reference to the number of error events that the product type / risk type point is exposed. By severity mean reference to the loss amount / potential loss amount that the operational risk event is exposed to when the risk event materializes.
- The classification of risk shall be made as High Frequency High Severity (HFHS), High Frequency Low Severity (HFLS), Low Frequency High Severity (LFHS) and Low Frequency Low Severity (LFLS).

*Handwritten signature and date: 2024/10/28*



For the identification, assessment and measurement of the operational risk, Bank shall use online models as Operation Risk Event Reporting and Branch Operations Risk Assessment and Profiling Indicators. Branches and Departments should record the events on the online module immediately of event taken place.

**a. Operation Risk Event Reporting and Risk Sharing Module**


Bank shall implement the online module Operation Risk Event Reporting for the measurement of risk identified in various branches/departments as follows:

- Operational activities which poses potential risk along with details at least including origin, causes, lapses, responsibilities and action taken by branch/departments, further action plan for mitigation of such risk identified by branches/departments shall be instantly reported to the higher authority through online module for the notification and correction.
- Operational risk identified in branches and departments are classified in various type such as Internal Error/Fraud, External Error/Fraud, System Failures/Error, Damage Physical Assets etc.
- Operational risk incident that could have possible impact on bank as defined in online module are cash excess/(short), accounting error, security hazards, confidentiality breach, technological errors, hacking, fake note/guarantee, CCTV/ATM problems, customer complaints, loss of banking assets, loss of key documents, disciplinary breaches, unauthorized access to system and customer account, insider trading, unethical use of banks position etc.
- The identified operational risk events shall be measured into high, medium and low risk level according to their risk severity and frequency.
- Operation Risk Management Department shall measure the operation risk event through using following risk matrix:

		SEVERITY				
		Negligible	Minor	Moderate	Significant	Severe
FREQUENCY	Very Likely	Low	Medium	High	High	High
	Likely	Low	Medium	Medium	High	High
	Possible	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	High
	Very Unlikely	Low	Low	Low	Medium	Medium

- Risk measurement of reported incident for overall bank shall be conducted on monthly basis and report to the higher management for their review and recommendation/instruction so as to mitigate such type of incident in future.
- The monthly incident reporting shall be shared with all branches/department so that proactive measure can be taken by branches to avoid such type of risk incident.

*Signature*  
2024/10/28



**b. Branch Operation Risk Assessment and Profiling Indicator Module**

Bank shall implement online module Branch Operation Risk Assessment and Profiling Indicator for quantitative measurement of the operational risk of the branch as well as bank as a whole. Operational risk activities shall be categorized into 11 group in which 53 risk indicators are self-assessed. Certain risk weight shall be assigned in risk indicators according to their severity for the measurement of the risk level. Followings are the group along with their risk weight in which bank shall categorize operational activities:

S.N.	Activities	Risk Weight
1.	Health, Safety & Security of Work Stations and Office Premises	0.1
2.	Customer Complaints and Customer Services	0.1
3.	Cash Management (Teller, Vault & ATM) Practices	0.15
4.	Cheque Payments and Cash/Cheque Deposit	0.15
5.	Customer Account, Documents and Confidentiality Maintenance	0.13
6.	Loan Operations and Credit Documentations	0.1
7.	Key Handling	0.02
8.	Account Monitoring and House Keeping	0.05
9.	ATM Management	0.05
10.	Compliance and Others	0.05
11.	Internal and External Audit Observations	0.1

Branch need to self-assess the operational activities according to the self-assessment risk indicator on monthly basis. Such assessment shall be conducted within 15 days every month. The risk level of the individual branch shall be calculated using following formula:

Total Operational Risk of each risk indicator = Weight given to each risk indicator X Risk severity for each condition


Total Operational Risk of Each Category = Weight given to each category X sum of total operational risk of each risk indicator in that category

Total Operational Risk of Each Branch = Sum of Total Operational Risk of Each Category

Total Operational Risk of Overall Bank = Sum of Total Operational Risk of Each Branch

According to the risk score obtained from self-assessment through risk indicator, individual branch will be categorized into following category:

*2024/02/28*



S.N.	Risk Weight Exposures	Risk Category
1	Up to 6	Inherent Risk
2	6 to 12	Low Risk
3	12 to 20	Medium Risk
4	20 to 30	High Risk
5	Above 30	Very High Risk

Branches shall be categorized in above mentioned five category according to the score obtained from self-assessment of the risk indicator. Likewise, operational risk level of the overall bank shall be calculated as follows:

Particulars	Average Score*	Number of Branch	Weight* **	Final Score***
Inherent Risk				
Low Risk				
Medium Risk				
High Risk				
Very High Risk				
<b>Overall Score****</b>				
<b>Risk Level</b>				
<b>Overall Score of Previous Month</b>				
<b>Risk Level of Previous Month</b>				
<b>Direction</b>				

$$\text{*Average Score} = \frac{\text{Sum of Total score of particular risk level}}{\text{Total Number of branch in that risk level}}$$


$$\text{**Weight} = \frac{\text{Total Number of Branch in particular risk level}}{\text{Total Number of Branch}}$$

$$\text{***Final Score} = \text{Average Score} \times \text{Weight}$$

$$\text{****Overall Score} = \text{Sum of Final Score of all risk level.}$$

Every month Bank shall calculate the overall operational risk score and risk level of the Bank. The movement of risk score and risk level shall be analyzed and control measures shall be implemented to mitigate the identified risk areas. Bank shall adopt low level of risk appetite for operational risk.

*Signature*  
2024/10/28





### 5.3 Risk Monitoring

Bank shall have the appropriate monitoring and reporting mechanism in place at the Board, Senior Management and business line levels to support the proactive management of operational risk. It offers the quickly detection and correction of 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 loss events. The risk monitoring shall cover Bank's entire range of operations and all types of material risks inherent in operations. The monitoring shall be undertaken with the following scopes:

- Monitoring shall be for all the significant business lines / functional lines.
- An effective risk reporting environment shall be established. Risk reporting shall be designed in tune of authorities and responsibility of board of directors, senior management and other staffs.
- Establish early warning signals (EWS) for managing risk of future losses. KRI could be used as EWS.
- While monitoring the available data, consideration shall be given to both internal loss data and external loss data.


### 5.4 Risk Control and Mitigation

Once risk is identified, assessed and measured, and the Bank decides to take the risks, these risks shall be controlled with a strong control environment in place through policies, processes, systems, internal controls, risk mitigations and / or transfer activities. Bank shall periodically review the risk limitation and control strategies and adjust the operational risk profiles accordingly using appropriate strategies, in light of the overall risk appetite and profile. Control activities will be designed to address the operational risks that have been identified. Those risks that cannot be controlled, bank decides whether to accept these risks, reduce the level of business activity involved or withdraw from this activity completely.

Bank uses sufficient risk mitigation tools and program to reduce the exposure to, or frequency and/or severity of such events. In general, bank shall undertake following mitigating methods:

- Establish a strong risk management culture in the Bank through formulation and implementation of policies, manuals and guidelines.
- Board and the Senior Management shall be responsible to reinforce a strong risk management culture in the Bank. Adequate training on operational risks shall be provided to related personnel.
- There shall be a system of effective internal controls.
- There shall be an appropriate segregation of duties; and staffs are not assigned conflicting responsibilities.

*Handwritten signature and date:*  
2024/02/28



- Adequate internal controls within the bank shall be supplemented by an effective internal audit function that independently evaluates the control system of the Bank.
- Ensure that actual losses do not exceed the maximum risk appetite on the operational activities.
- Establish disaster recovery and business continuity plans.
- Establish outsourcing guidelines to ensure that outsourcing risks are minimized and monitored on effective way.

## 6. Capital Measurement and Operational Loss Limit

Operational risk arising from breakdown in internal controls and corporate governance can lead to financial losses through error, failure of information technology, fraud or failure to perform in a timely manner or cause the interest of the bank to be compromised. This may erode the capital of the Bank. Therefore, in addition to having effective internal control mechanisms in place, maintaining capital to safeguard the bank from possible threat is a key to mitigating the impact of operational risk.

### 6.1 Capital Measurement

Capital Adequacy Framework, 2015 relating to Basel III requires the Bank to hold capital against the risk of unexpected loss that could arise from the failure of operational systems. As provided by NRB Directives, the bank shall be following the Basic Indicator Approach for Operational Risk measurements. Under the Basic Indicator approach, bank shall hold capital for operational risk equal to the average over the previous three years of a fixed percentage (denoted alpha) of positive annual gross income. However with enhancement in risk management practices, the bank shall resort to adoption of a more advanced version of capital requirements for operational risks.

### 6.2 Operational Loss Limits


Operational Risk Management Department shall maintain the database of operational risk losses and operational risk events. Such database shall clearly record the operational risk type along with probability of loss. In absence of complete data of risk events with loss amount for at least 3 years, operational loss limit is defined as equivalent to risk weight for operational risks as per BASEL III. Amount of risk weight for operational risks is derived on quarterly basis.

## 7. Risk Treatment Strategies

Upon identification of the operational risk along with their probability and impact, bank shall consider such risk into following four risk treatment strategies for controlling the operational risk.

PROBABILITY	High	Reduce	Avoid	
	Low	Accept	Share/Transfer	
	Low	IMPACT		High

2075/10/28





**7.1 Avoidance:**

Bank shall decide not to proceed with the operational activity that introduced the unacceptable risk, and shall choose an alternative more acceptable operational activity that meets business objectives, or choose an alternative having less risky approach or process.

**7.2 Reduce:**

Reduction means minimize the probability of occurrence of risk event by creating the safe environment ensuring that risk can be reduced such as: preparing policies / manuals / providing trainings to staff, taking conservative approach to undertake the business etc.

**7.3 Share / Transfer:**

This is the process of implementing a strategy that shares or transfers the risk to another party or parties, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk. Bank shall make aware the third-party accepting the risk of their obligation.

**7.4 Acceptance:**

Acceptance means taking calculative risk in a particular transaction. Risk is an integral part of the banking business. This strategy may also be relevant in situations where a residual risk remains after other treatment strategy have been put in place. No further action is taken to treat the risk, however, ongoing monitoring is required.

**8. Operational Risk Management Model**


The bank shall follow below mentioned three line of defense approach as an operational risk management model:

Line of Defense	Responsible Unit
First Line	Business / Functional units
Second Line	Compliance/ Risk Function
Third Line	Internal Audit

**First Line:** The first line of defense is the Bank's Business and Functional Units. This include front-line employees who are responsible for processing transactions and applying internal controls to treat the risks associated with those transactions. Employee at first line of defense have primary responsibility for day to day business transaction and risk management. They are also responsible for implementing corrective actions to address process and control deficiencies.

**Second Line:** The second line of defense is the Bank's Compliance and Risk Functions that provide independent oversight of the risk management activities of the first line of defense. The responsibilities of second-line defense include reviewing risk reports and validating compliance according to the requirements of risk management framework. Second line of defense is responsible for establishing policy and process for risk management, provide guidance and coordination among all functions, liaison between third line of defense and first line of defense, oversight over risk areas and bank's objectives.

2020/10/28



**Third Line:** The third line of defense is audit function of the Bank who report independently to the senior management charged with the role of representing the Bank's stakeholders relative to risk issues. The audit function regularly review the first and second line of defense activities and results, including the risk governance functions, to ensure that the risk management arrangements and structures of the Bank are appropriate and are discharging their roles and responsibilities completely and accurately. The results of reviews of these audit functions need to be effectively communicated to executive management and board of directors in order to take appropriate action to maintain and enhance the risk management culture of the Bank.

## 9. Risk Management Tools

The bank shall use the following tools for the effective management of operational risk. These tools serve as the fundamentals for identification, assessment and management of operational risk. These tools shall be deployed proactively in an anticipatory fashion to recognize and manage risk in forward looking manner:

### 9.1 Key Control Standards

Bank shall outlines the key control standards from control perspective. The minimum qualitative control standards to be attained by various business functions shall be outlined according to the functionality and complexity of the business unit. Key control standards shall be updated and revised taking into consideration of issues raised by Audit, risk reporting and risk assessment carried out by Risk Management Department. Some of the Key Control Standards are outlined in **Annexure-1**

### 9.2 Business / Functional Line Mapping

Bank outlines the business areas for mapping of business lines from control perspectives. Based upon the size, complexity and landscape of banking business, bank undertakes mapping the business lines and functional/support units. With sophistication and capacity enhancement, and use of better risk management tools, bank shall adopt business line mapping aligned with the Basel III requirements. In general, the business lines mapping will be as follows:

S. No	Business / Functional Lines	Areas
1	Business Banking	Project lending, real estate, export finance, trade finance, guarantees, corporate deposits etc.
2	SME and Consumer Banking	SME and Consumer lending and deposits including guarantees, card services, e-banking, other transaction banking services etc.
3	Payment & Settlement	Payments and collections, funds transfer, clearing & settlement, reconciliations etc.
4	Agency Service	Custody of assets, Custody of Information, Intermediary etc.
5	Accounting & Finance	Book keeping, accounting, financial management, budgeting, planning etc.
6	Information & Technology	IT, IT Infrastructure, Card, SWITCH, Storage, BCP, Disaster planning etc.

*Handwritten signature and date: 2024/02/28*



S. No	Business / Functional Lines	Areas
7	Human Resources & General Service	Human Resource Planning, Management, General Administration Management, Logistic Support etc.
8	Treasury	Interbank lending, placements, investments, etc.
9	General Operations	Business operations, customer servicing, corporate planning etc.
10	Others	As determined by Board / Management time to time

### 9.3 Key Risk Indicators (KRIs) / Early Warning Signals (EWS)

Bank shall determine key risk indicators (KRIs) and Early Warning Signals (EWS) which enable the Bank to identify current risk exposure and emerging risk trends, highlight control weakness and allow for the strengthening of poor controls and facilitate the risk reporting process. Such indicators shall be forward-looking and could reflect potential sources of operational risk such as rapid growth, introduction of new products, employee turnover, transaction breaks and system downtime and so on. When thresholds are directly linked to these indicators, an effective monitoring process can help to identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately. Some of the Key Risk Indicators (KRIs) and Early Warning Signals (EWS) are outlined in **Annexure - 2**


### 9.4 Contingency Planning

Bank shall have disaster recovery and business continuity plans to ensure its ability to operate as a going concern and minimize losses in the event of severe business disruption. The business disruption and contingency plans should take into account different types of scenarios to which the bank may be vulnerable and should be commensurate with the size and complexity of its operations. Management should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential.

### 9.5 Staff Training and Development Program

Bank shall have staff training and development program policy to ensure and enhance the competencies and productivity of the employee and improve the quality of product and services. Bank shall have prudent practice pertaining to training need assessment, planning for types / modes of training programs to be conducted, nomination of participants, post training evaluation of value addition achieved and other governing principles. Employees are the assets of the bank however, incompetent employees are the major factor for operational risk. Therefore, employee training represent an investment and will major tool for managing operational risk. Bank will focus on training of employee to ensure effective value addition to the Bank as well as individual employee in line with the corporate objective and individual career aspiration. Induction and orientation program shall be conducted to all newly recruited staff members of the bank before placing them in particular job function. Periodic online Knowledge Evaluation and Enhancement Program (KEEP) shall be executed to assess and enhance the knowledge and skill of the staff members.

*Signature*  
2024/10/28



## 9.6 Revenue Leakage Monitoring

Bank shall have revenue leakage monitoring unit which review and monitor the various aspect of revenue leakage. Unit shall monitor the various source of revenue on daily basis. Unit shall review and monitor following source of revenue on timely manner:

- |  |  |
|--|--|
| a. Good for Payment (GFP) cheque issue, GFP canceled | m. Draft/TT/Swift issuance   |
| b. Cheque returned due to lack of funds              | n. ABBS transaction  |
| c. Card issuance                                     | o. L/C and Guarantee issuance  |
| d. Re-pin issuance                                   | p. New loan disbursed and service charge                             |
| e. Mobile banking service renewed                    | q. Loan renewed and renewal charge                                   |
| f. Pin code regeneration for mobile banking          | r. Reversal on Income ledger   |
| g. Pin code regeneration for e-banking               | s. Comparison of income and expenses ledger balance                  |
| h. Stop payment instruction                          | t. Manual deduction of interest                                      |
| i. Balance certificate issuance                      | u. Revaluation gain/(loss) and Trading gain / (loss)                 |
| j. Account closed within six month of account open   | v. Comparison of standing tariff & commission charges of peer groups |
| k. Cheque presented through ECC                      | w. Locker rent   |
| l. IPS transaction                                   |  |

## 9.7 Turnaround Time

Bank shall have turnaround time for every service and product that is offered by the Bank. Every department and business center shall determine the turnaround time for processing and accomplishing the service. Each customer service turnaround time shall be determined and published in the website. The deviation in standard turnaround time with actual service delivery time will be analyzed and corrective measure will be implemented.


## 10. Basic Operational Risk Measures

### 10.1 General Banking

Management of Operational Risk start from the first line of defense. All day to day transaction must be executed considering the risk factor associated with such transaction. Bank shall ensure at least following measures in general banking services to manage the Operational Risk:

- All the policies, procedures and manual related to Cash, CSD, and Remittance shall be reviewed, updated and effectively implemented in a timely manner.
- Clear segregation of roles and responsibilities of the staff members executing general banking services
- There shall be dual control on all activities related to general banking such as maker and checker, compulsorily required two personnel and their signature in all external correspondence etc.

*Signature*  
2024/10/28




- Optimum use of fixed assets, vehicle, working place and other banking assets,
- Proper management of all documents related to account opening, closing, customer service, teller transaction and other general banking service
- Leave the office only after completing all activities related to that day and reconciliation of activities with output such as checking all teller till with transaction list, number of account opened with account opening document, number of GFP issued with GFP issuance register etc.
- Regular review and monitoring by supervisor such as verification of cash by BM/OI on surprise basis, checking all document for their completeness and correctness etc.
- Preparation and update of all register, forms and other correspondence as required by policies, procedures, manuals, circular
- Effective and adequate communication of information to upper level management

## **10.2 Information Technology System**

Effective use and sound implementation of technology may reduce Bank's susceptibility to some human errors, but increase its dependency on the reliability of information technology systems. Therefore, Bank shall have an integrated approach to identifying, measuring, monitoring and managing technology risks. Bank shall ensure at least following measures in IT function to manage the Operational Risk:

- All the policies, procedures, guidelines, manuals related to Information Technology and Security shall be formulated, reviewed, updated and implemented in a timely manner
- Bank shall have a sound information technology and security infrastructure that meets current and long-term business requirements in normal periods as well as stressed period to ensure data and system integrity, security and availability
- IT department shall have its own departmental structure having at least Development, Technology, IT Operation and Information Assurance Unit. Clear roles and responsibilities along with job description shall be provided to the staff members of the IT Department.
- Bank shall have an independent Information Security Officer (ISO) who is primarily responsible for reviewing, identifying, communicating and managing the IT risk as well as operational risk related to IT. He/she shall execute all responsibilities as depicted in Bank's IT and Security Policy. Further, the ISO will prepare an inventory of information assets throughout the Bank and an assessment of risk at each location.
- Bank shall formulate and implement at least E-mail Usage Policy, Internet Usage Policy, Network Usage Policy, Workstation & IT Assets Security Policy, Clean Desk Policy, Database & Data Center Security Policy, Password Policy and Data Retention & Disposal Policy to manage the IT risk as well as operational risk

*2024/02/28*



- Drilling shall be done as per the Bank's Business Continuity and Disaster Recovery Management Policy without fail.
- Bank shall conduct the penetration testing and ethical hacking test at least once in a year for identifying the vulnerabilities for all web application, network and core banking
- All staff members and IT personal shall fully comply with Bank's code of conduct to ensure the preservation of private information of Bank's customer, vendor, shareholder and all stakeholders
- Core Banking Software (CBS) as well as other application software, anti-virus application shall be updated regularly to fix the vulnerabilities and bugs.
- Bank shall use only licensed and trusted application software and implement firewall and anti-virus security
- Access to unauthorized personnel in Data Center shall be restricted. Security alarm, fire detection and suppression elements, access control mechanism, CCTV monitoring and power protection devices shall be implemented in Data Center
- Security awareness training shall be provided to all employee of the Bank at least once in a year.

### **10.3 Credit Administration Functions**

The primary responsibility of Credit Administration Function is preparation and execution of security document, facility implementation and other various monitoring and reporting activities. Bank shall ensure at least following measures in Credit Administration Function to manage the Operational Risk:

- Bank shall have separate Credit Administration Guidelines for controlling and effectively executing the credit administrative function. Such guidelines shall be regularly reviewed, updated and implemented
- For proper division of work, Centralized Credit Operation Department (CCOD) shall have its own departmental structure along with clear segregation of roles and responsibilities. Structure may contain Security Documentation (Preparation and Execution), Credit Operation (Limit Implementation), Reporting and Monitoring Unit.
- All the activities related to Credit Administration shall have dual control mechanism such as document preparation by one staff and verify by another staff, limit insert by one staff and approve by another staff, report generate by one staff and verify by another staff etc.,
- Signatures of borrowers and other concerned shall be obtained in presence of Bank's staff.
- Mortgaged / Remortgaged / Release / Thado Rokka / Registration and other legal correspondence shall be done at least by assistant level staff

*Handwritten signature and date: 2020/10/28*






- Before limit implementation, CCOD shall ensure the adequacy and availability of insurance, CIC report, correctness of Basel Code, Sector Code, Risk Grade and ensure that all required parameters are inputted in system
- All the legal and security related documents shall be kept in fire proof cabinet and there shall have two key panel to open such cabinet. Separate register detailing where such documents are kept shall be maintained. All area where legal and security documents are kept shall have CCTV monitoring, fire detector and suppressor, fire extinguisher and other security measures
- Information regarding approval of loan along with comments/remarks of approving chain shall be provided to respective branches through e-mail before implementing limit, renewing limit in system.
- Original approved document shall be provided within 15 days of approval to branches within inside valley and within 30 days of approval to branches outside valley.
- Security In\Out register shall be maintained to record the movement of security document. Register must include maximum days for which such document has been released and the expected date to be returned.
- Periodic review of insurance expiry date, expiry of drawing power, account overdrawn, limit expiry, business inspection report and working capital details shall be done by the Credit Administration Function.

#### **10.4 Human Resource Management Function**

Effective management of human capital and hiring efficient human capital is the major tool for operational risk management. Bank shall ensure at least following measures in Human Resource to manage Operational Risk:

- All the policies, procedures, guidelines, manuals, bylaws related to Human Resource shall be formulated, reviewed, updated and implemented in a timely manner
- Job Description (JD) shall be provided to all staff members of the bank while joining in new job function
- Induction and orientation program shall be conducted to all newly recruited staff members of the bank before placing them in particular job function
- Individual file shall be prepared for all staff members. All academic qualification documents, professional qualification documents, experience certificates, photograph, citizenship certificates, medical report and other required documents as per staff bylaws shall be kept in the individual file. These files shall be reviewed and updated on regular basis.
- All files related to staff shall be properly kept in fire proof cabinet. Any training and development program attended by staff shall be updated in such file.
- Periodic reconciliation of staff advance and other staff related expenses shall be done

*Handwritten signature and date:*  
2024/10/28



- Regular training and development program shall be provided to all staff members as per their function and requirement.
- Periodic online Knowledge Evaluation and Enhancement Program (KEEP) shall be executed to assess the knowledge and skill of the staff members and accordingly training and development program shall be prepared.

### **10.5 General Administration Functions**

General Administration Function of the bank is responsible for all procurement, maintenance and administrative work. Development in risk culture in this function is necessary for effective management of the operational risk. Bank shall ensure at least following measures in General Administration Function to manage the Operational Risk:

- Bank shall have separate General Administration Guidelines in addition to Financial Bylaws for controlling and effectively executing the general administrative function. Such guidelines shall be regularly reviewed, updated and implemented.
- All the administrative function shall have dual control function such as maker and checker, all external written correspondence with at least 2 signature
- Bank shall maintain list of all vendors for various services such as ATM, CCTV, IT, construction and renovation, printing and stationery. Such list shall be reviewed and updated regularly.
- Problem encountered in any functions shall be resolved immediately considering the importance and its impact on Bank's reputation.
- Functionality of all ATM machine, all CCTV camera, token machine & system etc. shall be monitored all the time and ensure that there is no service interruption. All CCTV camera must have good visibility, recording capacity at least for 90 days, night vision in sensitive area, coverage of all bank premises etc.
- Branch office premises and working environment must be adequate and safe in terms of health, air, lighting, security and overall environment along with unexpired fire extinguisher, alarm system, waiting seat, Air Conditioner, rest room etc.
- All assets of bank shall be safe and fully insured at any time against various risk as per their nature.
- All inventory of stationery item, forms and other goods shall be adequately maintained and properly recorded.
- Prepare and monitor logbook of the usages of vehicles, generator ensuring its efficient uses.

*Signature*  
2024/10/28





**10.6 Compliance Functions**

Compliance with regulatory provision, internal policies, procedures, manuals, guidelines, framework, product paper and other provisions is the tools for risk management. Bank shall ensure at least following measures in Compliance Functions to manage Operational Risk:

- Bank shall have separate independent Compliance Department which looks after compliance status of the bank. Bank shall have compliance policy which govern compliance structure of the Bank. Such policy shall be reviewed, updated and implemented on regular basis.
- KYC for all account shall be reviewed and updated in regular basis. Account shall be opened only after screening in various list such as sanctions list, black list, rejected list etc. Risk grading in all accounts after due care for the purpose of reviewing shall be given.
- Compliance and implementation status of all regulatory requirement, internal policies, procedures, manuals, guidelines, framework, product paper and other required provision shall be reviewed on regular basis. Further, implementation status of recommendation of internal audit, external audit, NRB inspection and other audit & inspection shall be reviewed on regular basis.
- Training and development program shall be conducted to all staff members of the Bank regarding KYC, AML/CFT, various policies, procedures and manuals to mitigate the operational risk that may arises due to insufficient knowledge and skills.

**11. Disclosure Requirements**

Annual report of the bank shall make a full disclosure of approaches followed by the bank for identification, assessing, monitoring, measuring and controlling operational risks. Material operational losses shall be reported along with the reasons for such losses and strategies adopted to ensure that such losses are downsized to an acceptable / manageable level. The statement shall also include changes in the operational risk management practices during the year.

**12. Implementation, Review and Updates**

This Policy will be effective upon the approval of BoD. This Operational Risk Management Policy & Framework shall be reviewed at least annually. The review shall include identification of current risk exposure, emerging risk trends, control measurements and response to changes to organizational environment, business circumstances, legal conditions or technical environment.

*Signature*  
2020/10/28



**Annexure-1: Key Control Standards****A. Organization**

- Up to date and approved organization chart showing all positions
- Clear and appropriate segregation of roles and responsibilities
- Updated delegation of Authority in line with Bank's Policies and appropriate and clear reporting lines
- Exercised dual control mechanism where appropriate
- Periodic review of job description to ensure that they are up to date and clearly reflect jobholders' current responsibilities
- Periodic review of employee succession plan and transfer and rotation plan to ensure the availability of knowledgeable and skilled staff in absence of current staff
- Duly recorded handover, takeover procedures during staff movements/resignation


**B. Compliance**

- Compliance with all laws of land, all regulatory and legal rules, regulatory ratios, reporting requirements
- Compliance with standards, legal and regulatory requirements in respect of Money Laundering prevention. Report to appropriate authorities as when suspect detected
- Trained all staff regarding KYC, AML/CFT to detect and prevent money laundering
- Analysis of impact of regulatory changes in existing norms
- Compliance with Employees Code of Conduct in respect of ethical standards, integrity and honesty
- Maintain customer and business confidentiality
- Periodic compliance checklist preparation and assessment.

**C. Human Resource**

- Defined roles and responsibilities with job description to all staff in consonance with the competencies of the staff members
- Right people at right place. Training and development program to all staff considering individual skills & performance, product and service knowledge, career progression plan, changes to business plans, job transfer and rotation and changes in transaction processing system
- Adequate and proficient staffing at branches, departments and other unit as per the business volume, level of expertise needed, target budget and level of work

014/010  
2024/02/28



- Proper succession planning and transfer and rotation in regular interval
- Safe and healthy working environment, motivational and encouragement plans and other short term and long term staff benefits plans
- Immediate recruitment / transfer in key management position
- Effective Know Your Employee policy and periodic review of past and present status of employee.

**D. Legal**

- Legal agreement with all externally sourced suppliers and services
- Securely maintain all legal document, agreements, contracts, permits etc. in fire proof conditions
- Annual review of all customer contract documents and confirm with Bank's standards, regulatory requirements
- Proper recording of documents and information related to litigation to Bank and by Bank.

**E. Products**

- Product development as per the product development program. Review from operations risk, credit risk, finance, market risk, technology risk, legal risk and compliance risk perspective before development and launch of new product
- Annual review of product and product development program so as to identify and assess whether they reflect accurate products' risk profile. Such review identify the alignment of product with regulatory compliance and defined risk appetite
- Keep all documents related to product that is offered to customer securely and with restricted access
- Review and Verification of all instructions from customers and authorized officers
- Document all inputs and amendments undertaken by designated staff regarding to product


**F. Contingency Planning**

- Effective policy regarding Crisis Management, Business Continuity and Disaster Recovery
- Regular testing of Business Continuity Plan and Disaster Recovery Plan
- Annual review and update of Crisis Management Plan, Business Continuity Plan and Disaster Recovery Plan

**G. Security and Protection**

- Adequacy in security arrangements and alarm system

*Handwritten signature and date:*  
2024/02/28



- 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

**H. Technology**

- Compliance with applicable Technology policies and standards to ensure all processing systems are secure and robust to prevent undue exposure
- No sharing of User ID and Password by employee between each other
- Unique password chosen by user themselves, compulsory change of password in certain interval, password having defined number of character with specific features
- Auto log off from the IT assets in certain interval
- Regular information system audit
- Regular penetration testing and ethical hacking testing
- Regular monitoring of usage of internet by employee and monitoring of websites visited by employee
- Review of user profile to administer consistent with Information Technology and Security Policy


**I. Audit**

- Approved Audit plan with appropriate milestones addressing all significant auditable unit
- Implement of all gaps identified by audit
- Coverage of all significant risk areas

**J. Finance**

- Adherence to prescribed Accounting Standards and local GAAP
- Timely reconciliation of assets and liabilities
- Exhibit monitoring, controlling and reporting
- Applicable policies, procedures and practices to be applied on the book keeping and financial preparation.

*Handwritten signature and date: 2024/02/28*



Handwritten signature and date: 2024/04/28



**Annexure-2: Key Risk Indicators (KRIs) / Early Warning Signals (EWS)****A. General Banking and Customer Service Related**


1. Substantial number of account opened with pending document, pending document to be collected since long
2. KYC of few accounts is reviewed and updated and substantial number of account still need to be reviewed
3. Huge number of accounts are opened in a single day by single staff
4. Large number of cheque printed but pending to delivered to customer by more than 90 days
5. Large number of ATM printed but pending to delivered to customer by more than 90 days
6. Regular and substantial number of customer complaints regarding service of the Bank
7. Large number of card transactions disputed by customer and remain open for long time
8. Same person is signatory in multiple account
9. Account operated without uploading signature specimen card in system
10. Increasing number of dormant account and dormant account activation
11. Increasing number of blocked account and number of blocked account activated
12. Regular reporting of counterfeit currency, forged cheques/drafts

**B. Cash and Vault Operation**

1. Frequent teller cash excess short report and failed to identify the reason for such events
2. Pending cash amount in Cash in transit
3. Frequent counterfeit note presented in counter
4. Large number of deposit slip and cheque without denomination, source not mentioned in deposit slip
5. Instances found where cheque was encashed without verifying signature
6. Instances found where staff has miss used the cash of the bank
7. Easy access to person other than teller staff in cash area
8. Vault opened by non-key custodian, entry of unauthorized person in vault area
9. Frequent payment of cheque and acceptance of deposit beyond teller limit
10. Teller staff use mobile phone most of the time while dealing with customer
11. Maximum cash note having small denomination
12. Use of vault key for a long time
13. Frequent mistake entry in customer account
14. Regular vault limit exceeded

**C. Reconciliation**

*Handwritten signature and date: 2024/10/28*



1. Long pending item in Inter Department and Inter Branch Account
2. Long pending and unreconciled amount in Nostro Account
3. Unidentified matured fixed deposit pending since long
4. Unidentified long pending amount in ATM and Teller
5. Unavailability of exhibit of financial accounts on regular basis
6. Unidentified and long pending item in Suspense/Adjustment Account
7. Long pending reconciliation of stock consumption, fixed assets, demand draft, MC payable

**D. Credit Administration**

1. Non-Performing Assets level beyond appetite level
2. Frequently loan approved without obtaining complete supporting document
3. Frequently failed to renew the insurance on time
4. Downgrade of pass loan in loss category
5. Substantial loan file forwarded from branch requesting waiver to comply with product paper, CPG
6. Large number of loan account in expired status, large number of loan accounts in overdrawn status
7. Huge number of loan file due revaluation


**E. General Administration and Security Arrangement**

1. Frequent ATM down time reporting
2. Frequent problem reporting in CCTV, lack of adequate CCTV recording capacity
3. Frequent problem reporting in electricity line and voltage fluctuate
4. Delay in refill of expired extinguisher
5. Frequent complaint from customer and staff regarding working station and overall environment of the bank/branch premises
6. Frequent delay in delivery of stationery item and other goods to branch and departments
7. Unprofessional behavior to customer by guards and allow the customer to enter into branch premises without checking properly
8. Frequent delay in renewal of insurance policy of the assets
9. Consumption of fuel beyond normal trend
10. Excessive use of office vehicle in personal purpose

**F. Information Technology**

1. Frequent server down reporting
2. Frequent network problem reporting

*Handwritten signature and date:*  
2024/10/28



3. Frequent hacking and penetration attempts report
4. Entry in system by one staff/customer using user ID and password of another staff/customer
5. Use of outdated system and application, pirated software and application
6. Failed to update the anti-virus and other application
7. Frequent delay in preparation of query in system as requested by users or preparation of mistake query
8. Easy access to the administrative right, no mandatory to scan the external device before use
9. Repeated complaints from customer regarding e-banking accounts compromised through phishing

**G. Human Resource**

1. Frequent and excessive staff turnover in the Bank
2. Frequent late attendance by staff members
3. Tendency of going to leave by many staff in same time
4. Frequent over time reporting
5. Problem in executing activities smoothly in absence some staff
6. No proper handover and takeover arrangement
7. No availability of complete document required while selection and recruitment process

**H. Compliance**

1. Large number of account opened without risk grading
2. Substantial number of Suspicious Transaction Reporting in short span of time
3. Frequent breach of Threshold Transaction limit
4. Substantial number of issues raised by internal audit, external audit and NRB inspection team yet to be complied/resolved
5. Frequent transaction by staff of the Bank in customer account

*Handwritten signature and date: 2020/10/28*





**Board of Directors:**

S.N.	Name	Position	Signature
1.	Mr. Upendra Keshari Neupane	Chairman	
2.	Mr. Iman Singh Lama	Director	
3.	Mr. Chandra Prasad Bastola	Director	
4.	Mr. Madhav Prasad Bhatta	Director	
5.	Mr. Krishna Shrestha	Director	
6.	Dr. Kailash Patendra Amatya	Director	

2075/10/28

