OPERATIONAL RISK MANAGEMENT POLICY

Table of Contents

1.0 Introduction....5
1.1 Definition and Categorization....5
1.1.1 Regulatory Compliance Risk:....5
1.1.2 Financial Crime Risk (FCR):....6
1.1.3 Legal Risk:....6
1.1.4 People Risk:....6
1.1.5 Physical Security & Safety Risk:....6
1.1.6 Operations/Business Resilience/Service Delivery Risk:....6
1.1.7 Technology Risk:....6
1.1.8 Third-party/Vendor Risk:....6
1.1.9 Financial Reporting & Tax Risk:....6
1.1.10 Product/Model/Process Management Risk....7
1.1.11 Information Security Risk....7
1.2 Policy Objectives....7
1.3 Principles For Managing Operational Risk (OR)....7
1.4 Scope Of Operational Risk Policy....8
1.4.1 Product approval process....8
1.4.2 Project Risk Management....9
1.5 Boundaries with other risk classes....9
1.6 Ownership, Review and Update....9
1.7 Dispensations for non-compliance....9
1.8 Unauthorized deviation....9
1.9 Related Documents & Process Changes....10
2.0 Governance....12
2.1 Operational Risk Governance Structure....13
2.2 Roles and responsibilities....13
2.2.1 The Board of Directors (BoD)....14

2.2.2 Risk Management Committee (RMC) 14
2.2.3 Chief Risk Officer (CRO) 14
2.2.4 Operational Risk Management (ORM) 15
2.2.5 Business Units (BU) 15
2.2.6 Audit Committee 16
2.2.7 Audit (Internal & External) 16
3.0 Operational Risk Appetite 19
4.0 Operational Risks Process & Tools 22
4.1 Operational Risk Identification/Capture 22
4.1.1 Event Identification 22
4.2 Operational Risk Assessment 23
4.2.1 Assess the Likelihood 23
4.2.2 Assess the Impact 23
4.2.3 Risk levels 24
4.2.4 Risk Classification 25
4.3 Operational Risk (OR) Management: Risk Response 26
4.3.1 Risk Acceptance Criteria 27
4.4 OR Monitoring 27
5.0 Operational Risk Management Methodologies 30
5.1 Risk and Control Self-Assessment (RCSA) 30
5.2 Internal loss data 30
5.3 Key Risk Indicators (KRIs) 31
5.4 Stress and Scenario Testing 31
5.5 External Loss Data 32
5.6 Issue & Action Tracking 32
5.7 OR Awareness & Culture 32
6.0 OR Reporting & Management information 34
7.0 Capital Assessment 36
7.1 Basic Indicator Approach (BIA) 36
APPENDIX 1: CATEGORIZATION OF OPERATIONAL RISK 37
DOCUMENT APPROVAL PAGE ..... Error! Bookmark not defined.

List of Tables, Figures & Equations

Table 3-1: Board High-level Statement of Operational Risk Appetite 19
Table 4-1: Operational Risk Likelihood Assessment Rating Scale 23
Table 4-2: Operational Risk Grading Matrix 24
Table 4-3: Overall Risk Rating & Descriptions 25
Table 4-4: Risk Responses/Treatment Options 26
Table 5-1: Operational Risk Loss Reporting Threshold Amount 31
Table 7-1: Basic Indicator Approach Guide 36

Figure 2-1: Operational Risk Management Three Line of Defense 12
Figure 2-2: Operational Risk Governance Structure 13

Equation 7-1: Basic Indicator Formular 36

1. INTRODUCTION

1.0 Introduction

This policy statement outlines Premium Trust Bank's strategy and objectives for operational risk management and the approach and processes by which the bank achieves those objectives.

The policy takes account of and is consistent with operational risk policy guidance issued by the CBN Prudential Guideline on Risk Management & the Basel III framework:

This policy has been approved by the Board of Directors and is applicable to all business units and functional areas, including Support Functions, finance, risk management, Legal services, personnel, operations and compliance divisions the bank. All managers and staff are expected to abide by the policies and rules set out in this policy statement.

1.1 Definition and Categorization

Premium Trust Bank has adopted the following definition of operational risk:

> ***"The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"***

Operational risk presents significant exposures to Premium Trust Bank, including potentially high-severity-low-frequency losses, such as catastrophic losses, which may threaten its survival and capital adequacy.

Premium Trust Bank has established a common risk language to provide a consistent framework for the definition and categorization of risk and the organization of its risk management activities. Within this framework, the Bank categorizes operational risk into the following sub-categories, as summarized below. See Appendix 1 for the detailed risk categorization as set out in the Bank's risk register.

1.1.1 Regulatory Compliance Risk:

The risk of loss, financial or otherwise, arising from a failure to comply with the laws, regulations, or Codes applicable to the financial services industry. Underlying causes of regulatory compliance risk can be one or more of the following:

1) Lack of understanding of laws and regulations
2) Misinterpretation of their meaning
3) Lack of awareness of regulatory change
4) Failure to communicate changes to all interested parties
5) Inadequate controls to ensure requirements are met
6) Failure to monitor procedural effectiveness

1.1.2 Financial Crime Risk (FCR):

The risk that the Bank will incur financial or reputational loss via association with money laundering, fraud, market abuse or similar criminal misconduct. The misconduct can be external or can be perpetrated by our own customers or employees. The loss can be direct (as in the case of fraud) or arise through legal or regulatory action.

1.1.3 Legal Risk:

The risk of unexpected loss, including reputational loss, arising from

1) Defective transactions or contracts.
2) A claim (including a defense to a claim or a counterclaim) being made or some other event occurring which results in a liability for the bank or other loss
3) Failure to protect the title to an ability to control the rights to assets of the Bank (including Intellectual property rights).
4) Non-compliance to a change in the law.
5) Jurisdictional risk

1.1.4 People Risk:

The risk of loss – financial, reputational, or otherwise, arising from a failure to manage the Bank's human capital resources. This includes Fraud Risk & Conduct Risk

1.1.5 Physical Security & Safety Risk:

The risk of failure to protect lives and property of the bank. This includes Health & Safety risk arising from exposure to workplace hazards.

1.1.6 Operations/Business Resilience/Service Delivery Risk:

This is a sub-set of the broader Operational Risk category and concentrates upon the potential for the Bank to incur financial loss as a result of inadequacies or failures in operations processes, systems or staff. Operations Risk additionally incorporates the risk arising from disruption of Operations activities caused by external events

1.1.7 Technology Risk:

The risk of failing to develop, implement or operate the Bank's technology platforms and solutions to meet stakeholder requirements. This includes Data Management issues.

1.1.8 Third-party/Vendor Risk:

All risks associated with the sourcing and procurement of all third-party goods and services, including outsourcing.

1.1.9 Financial Reporting & Tax Risk:

The risk of not accurately recording, analyzing or reporting financial information across the Bank. This incorporates both information for the use of external stakeholders such as

shareholders (the Annual Report and Accounts etc.) and internal stakeholders such as Business/Function management and the Bank's Executive Directors.

Tax Risk refers to any uncertainty of outcome regarding the Bank's tax position. This can refer to uncertainty around the application of tax law to situations, uncertainty around the facts of a situation or uncertainty arising from the operation of systems to produce tax results.

1.1.10 Product/Model/Process Management Risk

Model risk is a type of risk that occurs when a financial model is used to measure quantitative information such as a firm's market risks or value transactions, and the model fails or performs inadequately and leads to adverse outcomes for the firm. Process risk relates to inefficiency and ineffectiveness of business process which may then lead to financial, customer, and reputational loss.

1.1.11 Information Security Risk

Information security risk is the risk of an event or events occurring which result in a business' information being lost, stolen, copied or otherwise compromised (a "breach") with adverse legal, regulatory, financial, reputational and / or other consequences for the business. This risk would be specifically handled by the Information/Cyber Security Function in the bank.

1.2 Policy Objectives

Premium Trust Bank objectives for operational risk management are as follows:

1) All significant operational risks are identified, measured, assessed, prioritised, managed, monitored and treated in a consistent and effective manner across the organisation.
2) Appropriate and reliable risk management tools (including key risk indicators, loss databases, risk and control self assessments and stress and scenario testing) are deployed to support operational risk management, particularly management reporting, decision making and capital assessment.
3) All directors, management and staff are accountable for managing operational risk in line with the roles and responsibilities set out in this policy.
4) Compliance with all relevant legislation, regulatory requirements, guidance and codes of practice; and
5) Key stakeholders receive timely, dependable assurance that the organisation is managing the significant operational risks to its business.

1.3 Principles For Managing Operational Risk (OR)

The bank's Operational Risk Management Framework is designed based on the following key principles adapted from Basel II Practice:

1. The bank shall identify and assess the operational risk inherent in all material products, activities, processes, and systems. THE BANK should also ensure that before new products, activities, processes, and systems are introduced or undertaken, the operational risk inherent in them are subject to adequate assessment procedures.

2. The bank shall implement processes to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that support the proactive management of operational risk.

3. The bank shall have policies, processes, and procedures to control and/or mitigate material operational risks. THE BANK should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, considering their overall risk appetite and profile.

1.4 Scope Of Operational Risk Policy

The Operational Risk Policy of Premium Trust Bank shall cover all activities, products, systems, processes and people are exposed to Operational Risk and hence the ORM Policy shall apply to the Bank on an enterprise-wide basis. All prescriptions of the policy, without any exception have to be consistently followed by all the Business Units (BUs).

Although, certain specific personnel are designated with specific responsibilities in relation to the management of operational risk, all employees of the Bank shall comply with the operational risk policy guidelines while discharging their respective functions.

1.4.1 Product approval process

The introduction of new products, activities, processes and systems require assessment of associated operational risks by the Bank. All new product proposals (Liability-based products, digital offerings, excluding asset-based products which shall remain within the exclusive list of the **Management Credit Committee, MCC**) will be placed before the Bank's **New Product Committee** (**NPC**) for their review and approval.

All new product proposals will be subject to detailed assessment, considering their exposure to operational risk, technology risk, governance risk, strategic risk, reputational risk, compliance risk including any other material risk such product launches are likely to contribute to the Bank. The proposals for new product launches will be directed to the New Product Committee by the proposing business unit through the Operational Risk Management Department (ORMD).

1.4.2 Project Risk Management

Project risk management deals with managing the risk of sub-optimal project planning and management (project execution risk). Effective project risk management helps to minimize the risk of poor or less-than-optimal project outcomes (project result risk). Projects shall be appraised, and the add-on risks shall be evaluated on a case-by-case basis.

1.5 Boundaries with other risk classes

Premium Trust Bank determines the categorization of a risk event based on its primary cause. Premium Trust Bank therefore considers a loss event to be an operational risk event if it arose as a result of inadequate or failed internal processes, people and systems or from external events.

1.6 Ownership, Review and Update

The Chief Risk Officer and Risk Management Committee is responsible for the ownership of and periodic revisions to the operational risk policy.

The Board reviews and approves the policy statement on an annual basis in order to ensure that the policy remains aligned with Premium Trust Bank's overall business and risk management objectives, current or future planned changes in the operations of the Bank and the annual business plan.

On an ongoing basis, internal audit provides timely, objective assurance regarding the continuing appropriateness of the policy statement and the adequacy of compliance with the policy statement.

1.7 Dispensations for non-compliance

Dispensations for non-compliance with this policy statement must be documented and approved by the risk management committee (operating under delegated authority from the Board). Such dispensations are reported to the Board at its quarterly board meetings. Dispensations for significant non-compliance with this policy statement must receive prior Board approval.

1.8 Unauthorized deviation

All unauthorized deviations from the standards set out in this policy statement must be reported to the Chief Risk Officer, Risk Management Committee and the Board. Depending on the nature and severity of non-compliance, the issue may be a matter of disciplinary conduct.

1.9 Related Documents & Process Changes

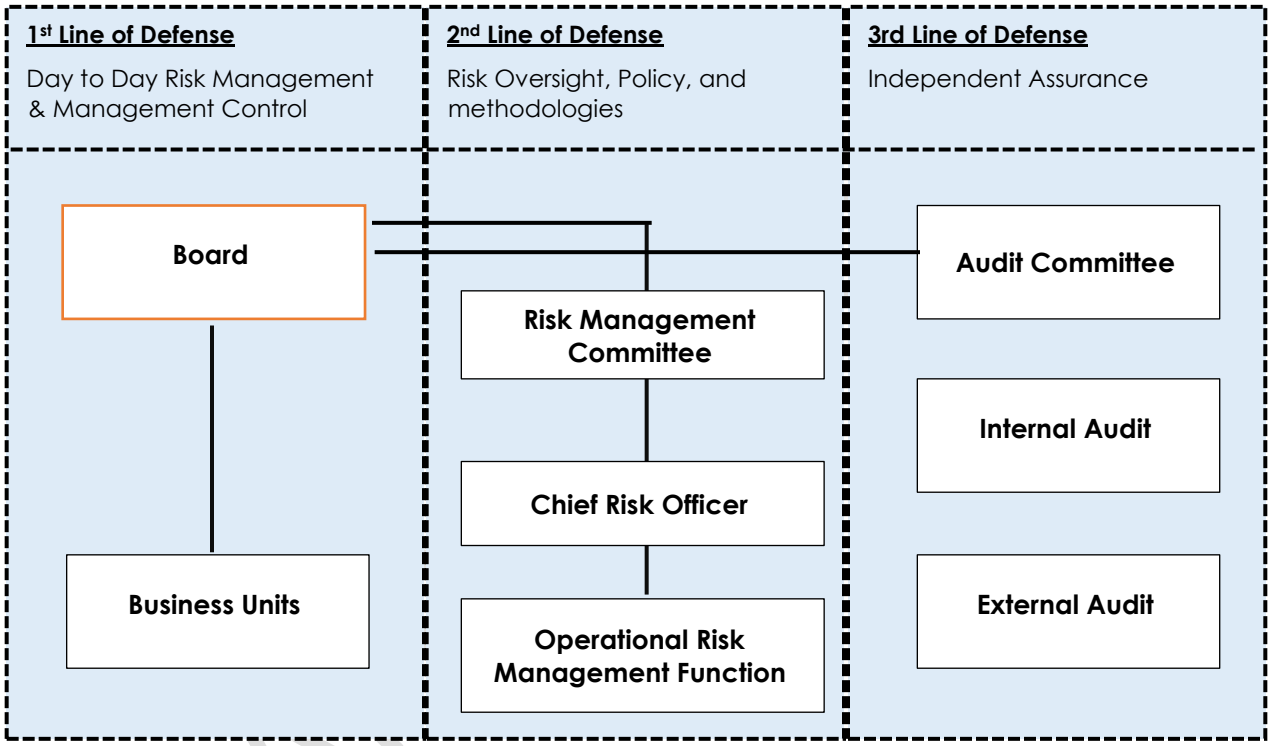
This policy should be read in conjunction with the bank's; Business Continuity Management Systems Policy, Enterprise Risk Management Policy, Operational Risk Management Standard Operational Procedure (SOP) manual and other Operational risk policies. All changes in the Operational Risk Policy must follow a strict change management process involving the above governance structure as well as the required attestation.

2. GOVERNANCE

2.0 Governance

The ORM framework provides the foundations and a common infrastructure for delivering, maintaining, and governing operational risk management. Premium Trust Bank has adopted a "three lines of defense" governance framework, as illustrated and explained below:

Figure 2-1: Operational Risk Management Three Line of Defense



The three lines of defense framework operates as follows:

- Staff in the first line of defense have direct responsibility for the management and control of operational risk (i.e., staff and management working within or managing operational business units and the Board).

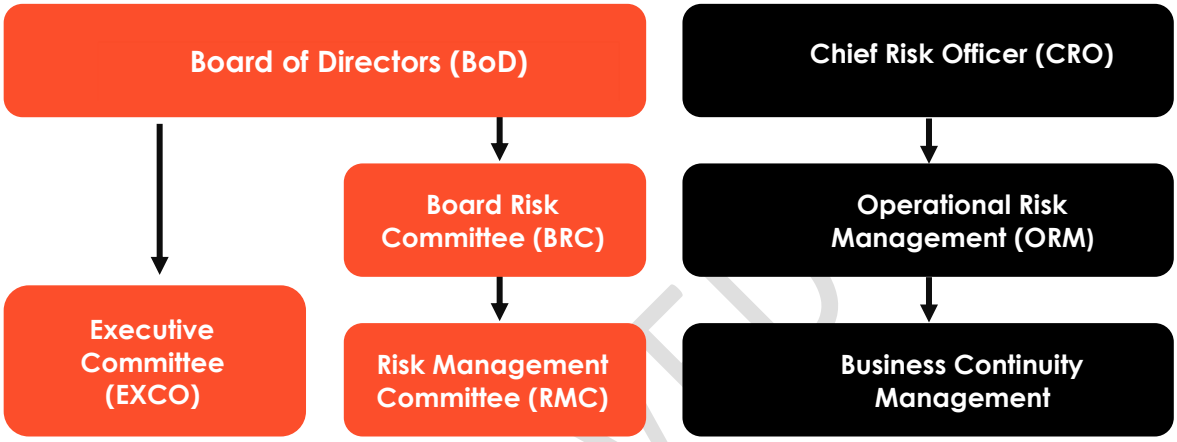
- Staff in the second line of defense co-ordinate, facilitate and oversee the effectiveness and integrity of Premium Trust Bank's operational risk management framework (i.e., the risk committee and enterprise risk management division); and

- Staff in the third line of defense provide independent assurance and challenge across all business functions in respect of the integrity and effectiveness of the operational risk management framework (i.e., internal, and external audit).

2.1 Operational Risk Governance Structure

The governance of operational risk shall follow the structure below:

Figure 2-2: Operational Risk Governance Structure



2.2 Roles and responsibilities

The overall responsibility for the Operational Risk of the bank resides with the Board. The responsibility of the day-to-day management has been delegated as described in this section. On a regular basis, the Board receives reports on THE BANK Operational Risk Profile.

To ensure consistency and prudent management of operational risks, the responsibility for managing operational risk has been split as follows:

- The overall governance owned by the Board Risk Committee (BRC) and Risk Management Committee (RMC)
- The approval of operational risk group policies and standards for risk identification, measurement, assessment, monitoring, and reporting is the responsibility of the Board Risk Committee (BRC) and EXCO.
- The operational risk management framework is owned by the bank's Operational Risk Management Function.
- The implementation of the operational risk framework within the Business Units and Control & Support Functions and the day-to-day management of operational risks is owned by their respective Line management and executed through their management structure supported by the members of the Operational Risk Management Function.

The roles and responsibilities for each of these functions/stakeholders mentioned above and referenced in three Line of Defense Model are described in detail below:

2.2.1 The Board of Directors (BoD)

The Board of Directors shall:

- Set the Bank's operational risk strategy and direction in line with the Bank's corporate strategy.
- Give final approval for the Bank's Operational risk management framework.
- Periodically review the Framework to ensure its relevance and effectiveness; and
- Ensure that senior management is performing their risk management responsibilities.
- Obtains assurance on risk management effectiveness & compliance with set risk policy
- Reports to stakeholders on risk management
- Approve public disclosures

2.2.2 Risk Management Committee (RMC)

- To carry out the first level review and challenging of developed operational risk policies and procedures,
- To translate what is sometimes perceived as a "form filling exercise", into a proactive discussion via senior management participation and decision making on existing and potential Operational Risks.
- To ensure senior management become aware of and more directly accountable for, Operational Risks in their jurisdiction.
- To manage significant Operational Risks where they originate, within the business / function.
- To ensure compliance with the Bank's Operational Risk policies and procedures.
- To ensure that Operational Risks identified within business are assessed in terms of implications for wider business risk and to ensure that the identified business risks are reviewed and reported accordingly through the Operational Risk reporting process.
- To assist the CEO/Managing Director manage ongoing Corporate Governance issues
- Proposes the approach to risk management, risk policies, risk appetite and monitors compliance to them

2.2.3 Chief Risk Officer (CRO)

- Develops risk management strategy, principles, framework and policy
- Implements appropriate risk management processes and methodologies
- Advises and coaches management and business units on risk management
- Monitors the application and effectiveness of risk management processes
- Co-ordinates appropriate and timely delivery of risk management information

- Exercising supervisory responsibilities over the operational risk management in addition to responsibility over market risk, credit risk and other key risk types.
- Approving all reports, operational risk policy proposals, recommendations, and other documents prepared by the operational risk management group before submission to executive committee, operational risk committees and board risk management committees

2.2.4 Operational Risk Management (ORM)

The bank's Operational Risk Management Function is independent of the Business Divisions, Departments/Business Units, Branches and Control & Support Units and reports to the Chief Risk Officer, a member of the Board Risk Committee

The core responsibility of the bank's Operational Risk Management Function is the development and implementation of operational risk management across the bank.
This entails:

- Drafting operational risk management policies, standards, processes, and procedures
- Developing, driving implementation and maintenance of the Operational risk management framework
- Developing and distributing tools, techniques, methodologies, common risk language, risk frameworks, analysis, reports, communication, and training
- Coordinating, aggregating, and facilitating operational risk management activities
- Monitoring operational risk profile; including accumulations of risk, trends, and risks from internal and external market changes
- Escalating high priority issues to senior management and Board
- Collating, challenging, and reporting on aggregate risk profile, control effectiveness and actions to Risk committees and Board
- Analysing Business Divisions, Branches, Departments/ Business Units and Control & Support Functions operational risk to derive emerging themes for the Bank.
- Defining yearly operational risk limit and appetite for the Bank, Business and Support units respectively; and
- Liaising with external parties e.g., regulators, analyst, external auditors, etc. on the bank's operational risk management practices.

2.2.5 Business Units (BU)

The Business Units and Control & Support Functions are the first line of defense in our operational risk management process. They own, manage and are accountable for the operational risks and controls in their respective areas. They have the following responsibilities:

- Implement and comply with the bank's operational risk related policies, procedures, processes, and tools in their areas

- Assess risks and the effectiveness of controls in line with documented risk policies and toolsets.
- Design, operate and monitor a suitable system of control
- Manage and review risk as part of day-to-day business activity
- Keep the banks Operational Risk Management Department fully informed of operational risk developments via timely ad hoc or regular reports and meetings.
- Identify, review, and assess the inherent operational risks in the context of the existing control environment and document decisions with regards to the required mitigating action or acceptance of the risk.
- Ensure potential operational risks in new businesses, products and services and processes within their business units are identified and mitigated.
- Appoints/nominate responsible persons within the Business Units and Control & Support Functions to carry out the following ad-hoc OpRisk activities among which are:
    a. Capturing of all Operational losses, events, and exposures on the OpRisk Solution (where applicable)
    b. Proper monitoring and rendering of Key Risk Indicators
    c. Prompt response to OpRisk RCSA administered on branch/department
    d. Reporting of cases of default/breaches
    e. Serving as the department's Business Continuity Champion

2.2.6 Audit Committee

- Monitors and reviews the activities of internal audit, ensuring that internal audit has the necessary resources and access to information to perform its role
- Ensures that the financial activities of the business are subject to independent review and external audit, appointing the external auditor and monitoring the independence, objectivity, effectiveness and cost effectiveness of the audit
- Reviews the half-year and annual financial statements and other formal announcements on financial performance and principal regulatory returns before submission to the board

2.2.7 Audit (Internal & External)

Internal audit shall:

- Provide independent assessment and evaluation of the Bank's Operational Risk Management Framework.
- Monitor Business unit and Support function's compliance with the Bank's operational risk policies.
- Assess the adequacy of the Bank's Operational Risk measurement methodology.
- Assess the effectiveness of the Bank's risk management and control process for operational risk; and
- Conduct an independent assessment and evaluation of the risk in Business unit's activities.

In addition to the above, the External Auditor shall:

- reports on risk and control process failings, including corporate governance weaknesses, if identified during the external audit.

3. OPERATIONAL RISK APPETITE

3.0 Operational Risk Appetite

The Board articulates statements of operational risk appetite, namely the amount of risk that is acceptable and/or unacceptable to Premium Trust Bank:

- Divisional heads and business unit managers interpret and cascade down more detailed expressions of appetite / limits for their division / business function; and
- Business functions interpret, apply and operate within these more detailed statements of appetite, with guidance from operational risk management function.

Premium Trust Bank articulates its risk appetite via a combination of **qualitative statements**, **limits and thresholds** – above which specific requirements are identified for escalation and approval; and key risk indicators – with identified tolerance levels and escalation points.

The Bank's operational risk appetite shall be set at a level that minimizes erosion of earnings or capital due to avoidable losses from frauds, system failure and other operational inefficiencies and disruptions.

Based on current earnings capacity and capital base, the Bank's operational risk limit and appetite shall be set in any case to be lower than the industry average. Business units and support functions operational risk limits and appetite shall be defined based on the bank's overall appetite by the Chief Risk Officer and communicated at the beginning of each financial year

The Board's high-level statement of operational risk appetite is set out below.

Table 3-1: Board High-level Statement of Operational Risk Appetite

Operational Risk Categories	Board level articulation
People	Premium Trust Bank employs sufficient, suitably skilled and experienced staff
	Staff roles and responsibilities are clearly defined
	Staff performance is reviewed, and training needs met
	Premium Trust Bank is an equal opportunities employer
	Premium Trust Bank has zero appetite for fraudulent activity
	Potential conflicts of interest are avoided and/or disclosed
Process	Premium Trust Bank has a low operational risk appetite for process failure

	Zero tolerance for high priority internal audit / regulator issues
	No single operational risk loss to exceed N50,000/ year
	Annual aggregate operational risk losses not to exceed 1% of Gross earnings per year
Systems	No more than 1 IT system outages per year for more than 1 hour
	No IT virus-caused outage
	Zero tolerance of IT & data security breaches
	Effective and tested Disaster Recovery Plan (DRP) to be in place
Operations & Business Resilience	Not Less than 1 IT Disaster Recovery Test must be carried out annually
	Very low appetite for business outages
	Effective and tested Business Continuity Plan (BCP) arrangements in place
Legal	Premium trust bank seeks contract certainty before all legal agreements are signed
	Minimum appetite for legal action against the bank
	Premium trust bank complies with all relevant legislation

4. OPERATIONAL RISK PROCESSES AND TOOLS

4.0 Operational Risks Process & Tools

The purpose of an integrated Operational Risk Management Process is the active and proactive identification, Assessment, mitigation, monitoring and reporting of all Operational Risks (OR).

All Divisions, Business Units, Control & Support Functions (Units), as well as the risk owners are responsible on an on-going basis to execute the operational risk process.

4.1 Operational Risk Identification/Capture

Operational Risks must be actively identified through Risk Management and Control processes established by the Business Units, Control & Support Functions via

I. The occurrence of Operational Risk Events (OREs) within the bank or externally within other financial institutions,
II. Reviews performed by Internal Audit, Regulators, or external Auditors,
III. Self-Assessments, Delphi sessions, Scenario analysis or Risk Workshop,
IV. Assessments/Due Diligences performed in connection with changes in processes, products, or changes in view of the division's business strategy (i.e., Acquisitions, New Product approvals, etc.).
V. Operational Risk Issues within THE BANK must be recorded and analysed through integrated Operational Risk Management Processes using the OR framework.

4.1.1 Event Identification

The Bank intends to systematically capture all operational loss events and allocate them to the specified business lines and loss event types. The Bank's operational loss data shall be considered as an integral part of the overall operational risk management framework and will be applicable to all activities and functions of the Bank viz. the business as well as support functions.

An event is an incident or occurrence emanating from internal or external sources that affects the implementation of strategy or achievement of objectives.

Event Identification has to cover all business activities and risk areas and must be systematic and comprehensive to ensure that critical or high risks are not excluded.

All identified risk events may have the dimensions as given in the table below to facilitate analysis and comparison of risks. Bank may choose to add more dimensions when necessitated. (Please refer to Operational Risk Loss Data Management Policy for full details.)

4.2 Operational Risk Assessment

All identified Operational Risks must be evaluated. Identified individual Operational Risks must be evaluated in view of their potential severity and likelihood of occurrence/ frequency according to the risk Matrix – to maintain a consistent Risk language in the bank. The documentation of the risk evaluation is mandatory, but not for immaterial Operational Risks classified as “unrated”.

OR Risk analysis within the OR process involves assigning a numerical value to the **LIKELIHHOD** and **IMPACT** of a risk.

These values are then multiplied to arrive at a classification level of **Very high, High, Medium, Low or Very Low** for the risk.

4.2.1 Assess the Likelihood

An estimate of the likelihood of a risk occurring must be made. This should consider whether it has happened before either to this organization or similar organizations in the same industry or location and whether there exists sufficient motive, opportunity and capability for a threat to be realized. The likelihood of each risk should be graded on a numerical scale of 1 (Low) to 5 (high). General guidance for the meaning of each grade is given in table below:

Table 4-1: Operational Risk Likelihood Assessment Rating Scale

Grade	Description	Summary
1	Rare	Not likely to occur in a 3-year timeframe. Only likely to occur in exceptional circumstances.
2	Unlikely	Not likely to occur more than once in 2-3 years.
3	Possible	Likely to occur in a 1–2-year (2) timeframe
4	Likely	Will probably occur in the next 12 months. It’s typical of operations of this type due to external influences.
5	Frequent	Has a high probability of reoccurring within 12 months

4.2.2 Assess the Impact

The impact assessment considers the effect of the identified risk in consideration of:

- ✓ Impact on financial viability
- ✓ Media impact
- ✓ Impact on staff
- ✓ Legal Implication
- ✓ Impact of breaching legal or regulatory requirements
- ✓ Impact on Customers

The impact of each risk should be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in the Risk Matrix below

Table 4-2: Operational Risk Grading Matrix

LIKELIHOOD OF OCCURRENCE	5-Frequent	Low	Medium	High	Very High	Very High
	4-Likely	Low	Medium	High	Very High	Very High
	3-Possible	Low	Low	Medium	High	Very High
	2-Unlikely	Very Low	Low	Medium	Medium	High
	1-Rare	Very Low	Very Low	Low	Medium	High
		1-insignificant	2-minor	3-moderate	4-significant	5-critical
IMPACT DEFINITIONS	Financial	Less than N100,000	>N100,000 <= N1,000,000	>N1,000,000 to <= NGN 10,000,000	N10,000,000 or <= NGN 100,000,000	Above NGN 100,000,000
	Customer	No impact on customer satisfaction/retention	Minor negative impact on customer satisfaction/ retention	Moderate negative impact to customer satisfaction/retention	Serious negative impact to customer satisfaction/ retention	Severe negative impact to customer satisfaction /retention resulting in negative referral.
	Staff/Employee	Event can be handled and resolved by staff or lower-level management	Event could be delegated to middle management for resolution	Event will require senior and middle management attention	Event will require the Board and senior management attention	Event will require Board and senior management attention
	Regulatory	Verbal warning from regulatory authorities.	Written warning from regulatory authorities but no penalty	Written warning and penalty from regulatory authorities	Penalty from regulatory authorities and suspension of top management staff	Withdrawal of operating license, which threatens the Bank's ability to continue as a going concern
	Reputational	No impact on reputation	Potential impact on reputation	Reputation is impacted in the short term	Serious diminution in reputation with adverse publicity	Permanent damage to reputation

4.2.3 Risk levels

The Risk level shall be assessed for 2 situations where pertinent:

Inherent risk: Assessment of risks assuming that no controls exist. Assessment of inherent risk is recommended as it provides a good understanding of the inherent risk of the activity.

Residual risk: Assessment of the risks after mitigation actions. For each possible mitigation measure a cost/benefit analysis shall be performed. Very High and High residual risks are unacceptable. Medium risks are tolerated and can be accepted. Low is acceptable risk. The residual risk will be in the acceptable (Medium or Low) risk area.

Analysis/evaluation of the difference between the inherent and managed risk can provide a good understanding of effectiveness of the existing controls.

4.2.4 Risk Classification

Based on the risk matrix above, there are 25 different combinations of Likelihood and Impact ratings which results in a 5-scale Inherent or residual risk rating. Each of the 5 final ratings in the risk matrix are explained below:

Each identified risk will be allocated a classification based on the combination of Likelihood & Impact (L,I) :

Table 4-3: Overall Risk Rating & Descriptions

Rating	Definition
Very Low	These risks are very insignificant and should be ignored in the context of the business objectives and/or value drivers impacted, but management shall monitor the risks and take appropriate action, as necessary, to prevent the risks from becoming material.
Low	These risks are not currently material in the context of the business objectives and/or value drivers impacted, but management shall monitor the risks and take appropriate action, as necessary, to prevent the risks from becoming material.
Medium	These risks do not exceed tolerance; however, they are important in the context of the business objectives and/or value drivers impacted. Management shall develop action plans that will ensure timely mitigation of the risks. Monitoring is required to avoid worsening situations.
High	Breaches risk appetite: escalated to Risk Management Committee (RMC), mitigation assigned to members of RMC. Also, escalated to MANCO
Very High	Not only breach Risk Appetite but also severely threatens organization's ability to continue operations. Invoke Business Continuity Plans

4.3 Operational Risk (OR) Management: Risk Response

Based on the results of the assessment of risk, the risk level is determined for the risks. Then the appropriate risk response is chosen from

I. avoid the risk,
II. mitigate the risk,
III. transfer the risk or
IV. accept the risk.

Desired Risk response can be achieved through several combinations of mitigation strategies:

- ✓ Reduce likelihood of occurrence (by e.g., implementing process controls, supervision);
- ✓ Reduce impact (e.g., by limits, power of attorney).

The choice of risk response is determined by the expected cost of implementing controls vis-a-vis the resultant benefit of risk reduction.

The responses are described below:

Table 4-4: Risk Responses/Treatment Options

Response	Description
Avoid Risk	In the event where the cost-benefit analysis proves that the benefit margin is less than the risk cost, considering all types of risk that includes operational risk, the Bank will opt to avoid such risks. However, the decision to discontinue the activity or not to initiate the activity in the first instance shall be approved by RMC taking into account the strategic objectives.
Mitigate/ Reduce Risk	The Bank shall adopt suitable measures that enable reduction in either the frequency of occurrence of a loss event or in severity of impact due to the loss event. The Bank shall adopt sound internal controls to mitigate operational risks.
Transfer Risk	• Where the internal control environment does not specifically provide the support for reduction or controlling the risk, the Bank shall decide on transferring such risks primarily through insurance and outsourcing • Further, the above decision shall also take into account the cost associated with such mitigation. Cost shall not be higher than the expected loss on account of the activity in which the risk has been identified. The risk appetite of the Bank shall also be taken into

	account while implementing the risk transfer through insurance and outsourcing. • Where it is possible to share the risks between the Bank and the third party, the same shall be explored and implemented. • Any undesirable effects that could arise on account of risk transfer shall also be identified and accounted for at the time of decision by the appropriate authority.
Accept Risk	The Bank shall accept the residual risk after mitigating actions have been taken to resolve or control the original risk estimated from risk assessment-sessions, product review process, project or other risk self-assessment sessions, policy, KRI-reports, and audit findings.

4.3.1 Risk Acceptance Criteria

All identified Operational Risks rated Very high, High, or Medium prior to mitigation would be accepted when any one or combination of the following conditions are satisfied:

- ✓ the level of mitigation (i.e., the difference between the Inherent risk and the residual risk) is deemed sufficient by the Line Management (Expert Opinion)
- ✓ the duration of implementation of the mitigation strategy is adjudged by all parties to be reasonably sufficient
- ✓ and the residual Operational Risk rating after mitigating actions is lower than the Inherent risk rating

All accepted Operational Risks must be reviewed and documented annually with material changes of the accepted residual Operational Risk requiring the renewal of the risk acceptance approval.

Risk acceptances need to be signed off by:

- ✓ The Risk Owner,
- ✓ The Risk bearing unit
- ✓ The Impacted Divisions and Control & Support Units,
- ✓ The Lead, Operational Risk

4.4 OR Monitoring

Escalation, Reporting and Monitoring of Operational Risk must be sufficiently transparent, timely and actionable. Identified mitigating actions need to be traced to solution.

- ✓ OR monitoring will be a continuous process to measure and evaluate the effectiveness of the internal controls, to determine whether the risks are within the norms for risk appetite, and in line with the expectation levels, and to determine whether policies, procedures and regulations are adhered to.

- ✓ Monitoring shall be performed through various techniques that are supported by automated or other tools, Key risk indicators monitoring, action tracking, key control testing, (direct) supervision, quality assurance, back-testing, policy review or self – assessment
- ✓ Both the design and operating effectiveness of a control shall be subject to monitoring by various techniques. Monitoring of the design effectiveness shall help ensure that controls are defined for each risk, and that the design is effective

5. OPERATIONAL RISK MANAGEMENT METHODOLOGIES

5.0 Operational Risk Management Methodologies

In order to meet its operational risk management objectives, each business function within Premium Trust Bank is required to identify, assess, measure and control its operational risk in line with the policy set by the Board.

The following tools and techniques are used by each business unit, in line with the nature and scale of the business risks.

5.1 Risk and Control Self-Assessment (RCSA)

RCSA is a key component of Premium Trust Bank's operational risk framework and involves, on a quarterly basis, each business unit within the bank proactively identifying and assessing its significant operational risks and the controls in place to manage those risks.

RCSA is intended to add value to the Bank by providing a prioritised assessment of the significant risks and controls to its business objectives, which:

- ✓ draws on the input of management and staff across the bank.
- ✓ draws on the output of loss event data, key risk indicators and stress and scenario testing (see below).
- ✓ is updated quarterly, by means of a series of assessment workshops, meetings or questionnaires.
- ✓ focuses on the root causes of risk, rather than just its effects.
- ✓ draws on the bank's common risk language and categorisation for risk in order to analyse and aggregate the results of the self assessment; and
- ✓ allocates ownership or accountability to the key risks and related controls to managers and staff best placed to manage them.

The results are reported as part of quarterly management reporting, collated by the risk operational management function.

5.2 Internal loss data

The tracking of internal loss event data is a key component of Premium Trust Bank's Operational Risk framework. Internal loss events are categorised into actual loss, potential loss and near miss events as
follows:

- ✓ **Actual loss** – an incident that has resulted in a financial loss
- ✓ **Potential loss** – an incident that has been discovered, that may or may not ultimately result in a financial loss; and

- ✓ **Near miss** – an incident that was discovered through means other than normal operating practices and through good fortune or focused management action resulted in no loss or a gain.

Premium Trust Bank has applied the following thresholds for loss event recording:

Table 5-1: Operational Risk Loss Reporting Threshold Amount

Loss Type	Reporting Frequency to RMC	Threshold Amount
Actual Loss	Monthly	>/= NGN 10,000
Potential Loss	Monthly	>/= NGN 50,000
Near Miss	Monthly	>/= NGN 100,000

Sources of loss events may arise from: a new risk to the bank; and/or a lack of control/control failure surrounding a known risk.

In either case, loss events should be fed into the next self assessment exercise to identify any corrective action which may be necessary.

5.3 Key Risk Indicators (KRIs)

KRIs are measures which track the risk profile of Premium Trust Bank. Each business unit within the bank develops and monitors key risk indicators for its significant risks, which are:

- ✓ Target key operational risk exposures for the business unit
- ✓ Enable management of the underlying causes of risk exposures.
- ✓ Use thresholds aligned to premium trust bank's risk appetite and enable risk-based decision making
- ✓ Are monitored with a frequency that matches the nature of the risks
- ✓ Compliment the self assessment and loss event collection processes; and are reported as part of monthly management reporting.

5.4 Stress and Scenario Testing

Premium Trust Bank analyses the impact of unlikely, but not impossible events by means of scenario analysis, which enables the Management to gain a better understanding of the risks that it faces under extreme conditions:

- ✓ Scenario analysis is the process of evaluating the impact of specified scenarios on the financial position of the bank;
- ✓ both historical and hypothetical events are tested; and
- ✓ Scenario analyses are conducted at least annually, or more often if there is a change in the operations or operating environment.

Scenario analysis results are also an important input to the determination of the bank's regulatory and economic capital for not only operational risk but all Pillar 1 & II risks in Premium Trust Bank's business (see section Capital assessment).

5.5 External Loss Data

An external loss database potentially provides an indication of the size and spread of losses experienced by other banks and thus a wider frame of reference when assessing potential exposures as part of the quarterly self assessment exercise. Each business unit is therefore encouraged to collect and periodically monitor relevant external loss data.

5.6 Issue & Action Tracking

All the business support functions are subject to audits initiated both internally and externally via internal and external auditors. Similarly, observations arise as a result of risk assessments, KRIs, loss events etc. Issues could arise from, Project risk assessments, Scenario analysis and Product risk assessments. etc.

In order to render the risk and control assessments, KRI tests, loss events management at all levels more manageable and transparent, ORM Function shall keep track of the status of the outstanding items with relevant timelines agreed

ORMF shall monitor the observations resulting from Risk Assessments (like RCSA's, fraud), KRI-reports, Loss events, involvement in projects, Product Approval Process, Physical and Personal Security reports or other relevant sources for effective closure.

5.7 OR Awareness & Culture

Risk information shall be gathered, analyzed, and communicated in a structured way to ensure the relevant people in the Bank, management and staff are aware of the risks and take their responsibility for managing the risk. The Bank shall perform periodic local campaigns, targeted at all personnel across the Business Units to spread operational risk awareness.

6. OPERATIONAL RISK REPORTING AND MANAGEMENT INFORMATION

6.0 OR Reporting & Management information

Premium Trust Bank's Operational risk management function oversees the collation, aggregation, and analysis of business unit management information and challenges it prior to submission to the Risk Management Ccommittee RMC, and the Board.

ORM Function shall design Bank wide operational risk reports and dashboards. The reporting structure shall have adequate granularity and coverage of business units. Operational Risk reports shall be compiled and generated by ORM and addressed to, Senior Management and to the Board of Directors on a periodic basis. Information provided in such reports shall be used by senior management to make informed decisions in the prioritization of risks enterprise wide.

To achieve the, ORM Function shall require monthly management information from each business unit in respect of:

- ✓ loss events, near misses and potential losses.
- ✓ key risk indicators.
- ✓ risk profile.
- ✓ new or significantly changed risk exposures.
- ✓ key risks with significant control weaknesses.
- ✓ deviations from the risk policy; and
- ✓ overdue agreed action for treating significant risks and
- ✓ any other information that may be necessary

Premium Trust Bank requires immediate escalation to the Operational Risk Management Committee and Board in the following instances:

- ✓ unauthorised deviations from any of the standards set out in this risk policy statement; and/or
- ✓ likely or actual breaches of thresholds agreed by the risk committee, Premium Trust Bank Board and risk management function.

7. CAPITAL ASSESSMENT

7.0 Capital Assessment

Under the Basel II Accord, capital shall be earmarked to absorb expected operational losses and to protect the Bank against unexpected losses that may be encountered in the normal course of business.

- ✓ Banks were expected to commence a parallel run of both Basel I and II minimum capital adequacy computation with effect from January 2012.
- ✓ The minimum capital adequacy computation under Basel II rules commenced in June 2014.

7.1 Basic Indicator Approach (BIA)

BIA allocates operational risk capital using a single indicator, gross income, as a proxy for the institution's overall operational risk exposure. Banks using this approach must hold capital for operational risk equal to the average of a fixed percentage of annual gross income over the previous three years (this percentage has been set at 15% by the Basel Committee). Gross income is defined as net interest income plus net non-interest income.

There are no qualifying criteria for BIA, as it is meant to be applicable to any Bank, regardless of the Bank's sophistication or complexity.

The charge may be expressed as follows:

Equation 7-1: Basic Indicator Formular

$$(KBIA) = [\ \Sigma\ (GI1\text{-}n\ X\ \alpha))]/n$$

Table 7-1: Basic Indicator Approach Guide

Abbreviation	Description
KBIA	The capital charge under the basic indicator approach
GI	Annual gross income, where positive, over the previous three years
N	Number of the previous three years for which gross income is positive
A	15%, which is set by the Basel committee, relating the industry wide level of required capital to the industry wide level of the indicator

CBN has issued guidelines for the regulatory capital measurement and management framework for the implementation of Basel II/III. Premium Trust Bank will adopt the BIA to compute minimum capital for operational risk. The capital assessment methodology is addressed in more detail in the bank's Annual Internal Capital Capital Adequacy Assessment Process (ICAAP) Report.

APPENDIX 1: CATEGORIZATION OF OPERATIONAL RISK

Level 1	Level 2
People	Breach of employment legislation or regulatory requirements
	Ineffective employment relations
	Inadequate workplace safety
Fraud	Third-party/Vendor fraud
	Agent/broker/intermediary fraud
	First party fraud
	Internal fraud committed against the bank
	Internal fraud committed against customers/clients
Physical Security & Safety	Damage to the bank's physical assets
	Injury to employee or affiliate outside workplace
	Damage or injury to public assets
	Health & Safety Issues at Work
	Armed Robbery/Burglary
Operations: Transaction Processing & Execution	Processing/execution failure relating to clients and products
	Processing/execution failure relating to securities and collateral
	Processing/execution failure relating to third parties
	Processing/execution failure relating to internal operations
	Inadequate transaction execution, completion & settlement
	Inadequate account reconciliation
Conduct	Insider Trading
	Anti-trust/anti-competition
	Improper market practices
	Presales service failure
	Post sales service failure
	Client mistreatment/failure to fulfill duties to customer
	Client account mismanagement
	Improper distribution/marketing
	Improper product/service design
	Whistle blowing
	Breach of code of conduct and employee misbehavior
Financial Crime	Money Laundering and Terrorism Financing
	Sanctions Violations
	Bribery and corruption
	KYC and transaction monitoring control failure
Regulatory Compliance	Ineffective relationship with regulators
	Inadequate response to regulatory change
	Improper licensing/certification/registration
	Breach of cross border activities/extra territorial regulations
	Third Party management control failure

Third Party/ Vendor Management	Third-Party criminality/con-compliance with rules and regulations
	Inadequate intra-group agreement/SLAs
Information Security	Data Theft/malicious manipulations of data
	Cyber risk events
	Data privacy breach/confidentiality mismanagement
	Improper access to Data
Statutory Reporting & Tax	External financial and regulatory reporting failure
	Tax payment/filing failure
	Trade/Transaction reporting failure
	Inaccurate / incomplete management information
Data Management	Unavailability of data
	Poor data quality
	Inadequate data architecture/It Infrastructure
	Inadequate data storage/retention and destruction management
Product/Model/Process Management	Usability Issues
	Poor product support
	User adoption Issues
	Poor product design/product flaw
	Failure to identify or manage product risks
	Market rejection
	Model/methodology design error
	Model implementation error
	Model application error
	Change execution failure
	Lack of proper due diligence
	Lack of Segregation of Duties
Technology	Hardware failure
	Software failure
	Network / telecommunications failure
	Third party IT provider failure
	Inadequate virus protection
	Inadequate system security / information management
	Insufficient processing capacity
	Insufficient / untested disaster recovery processes
	Inadequate system upgrade management
	Inadequate control over outsourced activities – IT / finance
	Inaccurate / incomplete management information
	IT Change Management failure
Business Continuity/ Resilience	Inadequate business continuity planning/event management
	Natural disaster / catastrophic loss

	Man-made disaster / catastrophic loss
	Third party / supplier failure
	External theft or fraud
	External breach of system security
	Terrorist attack / denial of access to building
	Power outage
Reputational	Breach of banking license
	US or other overseas regulatory action
	Identify theft / abuse of brand
	Rating downgrade
	Corruption, intimidation, or coercion of staff
	Failure to comply with CBN legislation
	Regulatory breach, fine, bad press
Legal	Customer dispute; Litigations
	Dispute over service level agreements
	Public and employers' liability
	Breach of fiduciary duty
	Change in law / failure to interpret law correctly
	Mishandling of legal processes
	Contractual rights/obligation failure
	Non-contractual rights/obligation failure
Strategic	Adverse insurance cycle developments
	Technological developments in trading platform and distribution
	Adverse political developments
	Adverse developments in the wider economy
	Failure to manage change
	Failure to deliver business strategy

The end