LOSS DATA MANAGEMENT POLICY

Table of Contents

1.0 Introduction 2
1.1 Rationale for the Management of the Loss Database 2
1.2 Policy Scope 2
1.3 Policy Ownership 2
2.0 Definitions Key Terms 3
3.0 Database Structure 5
4.0 Loss Reporting 6
5.0 Roles and Responsibilities 7
6.0 Other Issues 8
7.0 Amendment and Exceptions 8
8.0 Policy Review 8
Appendix I: Loss Definitions 9
Appendix II: Basel Event Classification 0
Appendix III: Costs to be Included & Excluded in estimating OR Loss Amount 8

1.0 Introduction

The tracking of operational loss events is an essential pre-requisite for the development and functioning of a credible operational risk measurement system. Specifically, Basel II requires banks to develop policies for the collection of operational loss data across the enterprise.

For the purpose of definition, Premium Trust Bank shall recognise losses resulting from operational risk as the financial impact associated with an operational event that is recorded in the institutions financial statement consistent with generally accepted accounting principles. Financial impacts include all out-of-pocket expenses associated with an operational risk event but does not include opportunity costs implemented to prevent subsequent operational losses.

1.1 Rationale for the Management of the Loss Database

The maintenance of a loss database is important for the following reasons:

1) The data forms the basis for quantification of operational risk and shall also be used for the calculation of **capital charge requirement**.

2) To create or enhance awareness at multiple levels of organization. A basic understanding of exposure and loss experience is a prerequisite for comprehensive and effective risk management. A record of losses, accumulating into an aggregated picture of the losses per year by risk and business, provides the baseline for analysis and the value proposition for improvement.

3) The data shall be used for empirical analysis, to determine what is happening, what events are repeating, what products are affected, what control points are failing and what locations were affected. This analysis can help direct corrective action to improve the control environment.

1.2 Policy Scope

This policy document is meant for the activities of Premium Trust Bank only. The contents are binding on all staff (in their respective Business or Support Function and other auxiliary members of the workforce).

1.3 Policy Ownership

This document is owned by operational risk management department of the bank

2.0 Definitions Key Terms

2.1 Operational Risk Event ('Event')

An operational risk event (known as “Event”) is a specific incident that results from the failure or inadequacy of any drivers of operational risk (namely; people, process, systems or external events) and gives rise to one or more operational risk effects (namely; financial loss, penalties, impairment to future earnings e.t.c) . Operational risk events are currently classified in seven event type categories (Operational Risk Event Categories).

The events that caused, or potentially could have caused (near miss events) a material loss to the bank are covered under the definition.

2.2 Cause

The proximate Cause of an Event is the action or set of circumstances that led to the event. Causes seek to identify the action (or inaction) of an individual or institution or the incidence of a natural disaster that triggered, has a direct and most substantial impact on, and is a necessary condition to the occurrence of the Event.

2.3 Rapidly Recovered Loss

Rapidly recovered loss event shall mean an operational risk event that generates a loss that is completely or partially recovered within five days of the occurrence of the event;

2.4 Boundary Events

The term "Boundary Events" is used to refer to Events that might be categorized as Credit, Market, Insurance, or Strategic / Business risk on the one hand and/or Operational Risk on the other.

2.5 Potential loss

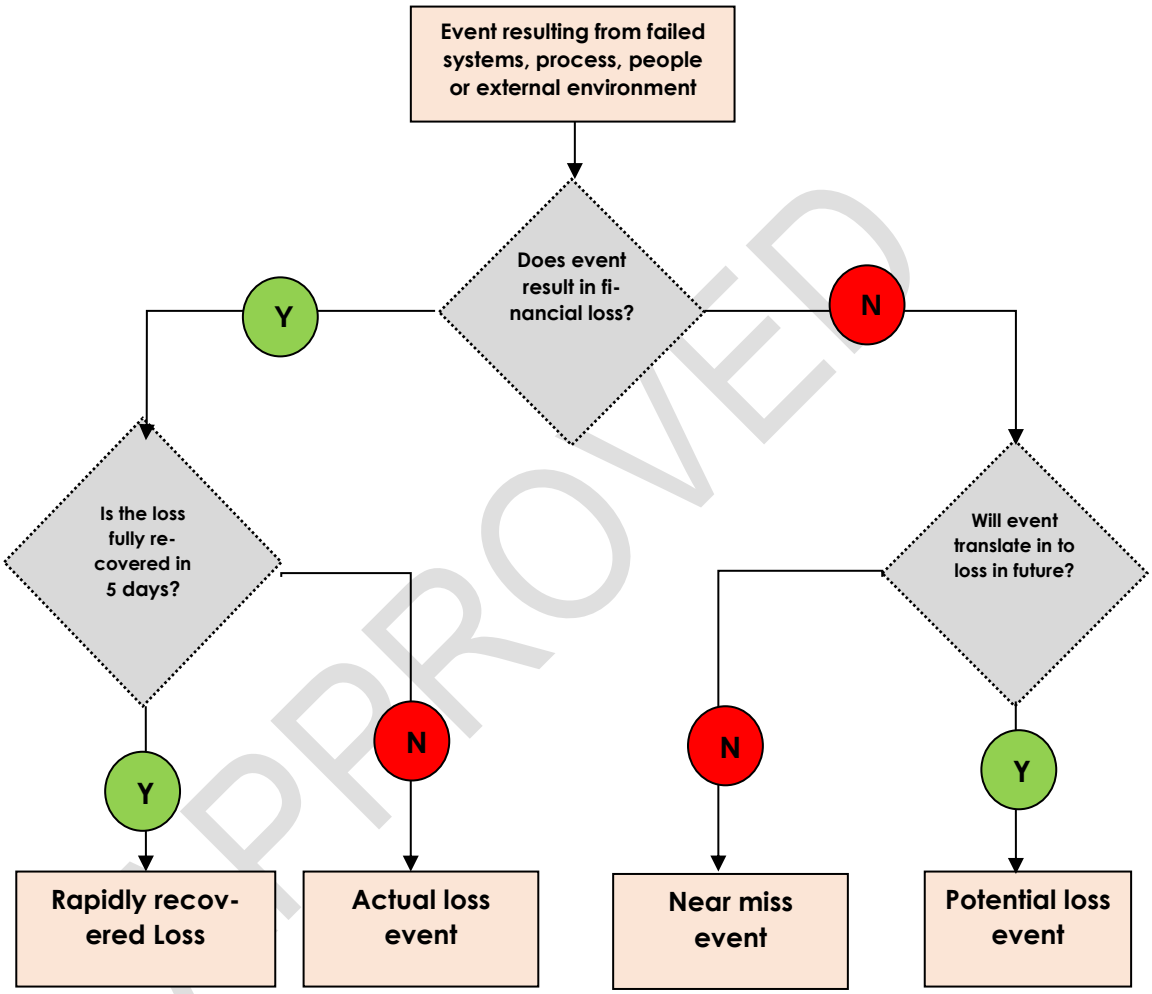
The potential loss amount is the amount that would be lost, if the development of the particular event has been less favorable and it reflects a pessimistic estimate of the actual total loss amount. Examples:

- Events prevented by non-standard or accidental checks; the potential loss amount then is the loss that would have occurred had the event not been prevented.

- More shares bought for a client due to a misunderstanding; Bank makes a profit on the deal; the potential loss is the amount that has been gained.

Loss Event Procedure Classification Flowchart

Figure below describes the flowchart depicting the classification procedure of loss events



See Appendix II for definition of Event Classifications as referenced in the flow chart above

3.0 Database Structure

The database shall contain the following information per event.

a) Date loss occurred
b) Date loss discovered
c) Loss event description
d) Contributing causes
e) Loss categories (guided by the Basel categorization of losses. i.e. Level 1 & 2)
f) Loss amount
g) Loss type (Actual loss, Potential loss, or Near Miss)
h) Recoveries (Operational and insurance separately identified)
i) Department/Branch/Business unit where the loss occurred
j) The business line to which the loss shall be mapped.

4.0 Loss Reporting

The loss reporting within Premium Trust Bank shall be premised upon the following principles:

4.1 All Losses shall be reported following the Basel Event Classification. See Appendix II for reference.

4.2 All loss amounts from NGN 10,000 (Ten Thousand Naira) and above must be reported and captured in the database, except for fraud related losses, for which all amounts (including amounts less than N10,000) must be captured in the database.

4.3 Market risk losses shall not be captured in the database. However losses due to policy infringements such as unauthorised trading and events of exceeding limits shall be regarded as operational risk losses and hence, must be reported and subsequently captured in the loss database. See Appendix III

4.4 Credit risk losses shall not be captured in the loss database. See Appendix III

4.5 All potential losses and near misses with no loss amounts shall also be reported and captured in the loss database (See appendix I for the definition of these terms and see appendix III for inclusions & exclusions

4.6 Any incident that leads (or could lead) to a loss should be reported within forty-eight (48) hours of detection of the loss event.

4.7 Other losses (e.g. litigation and replacement costs) should be reported in the loss database. See Appendix III

4.8 All loss reports emanating from any Branch/Department/Unit of the Bank shall at the minimum, contain the following details:

a) Date loss event occurred
b) Date loss event discovered
c) Description of the event
d) Loss amount
e) Recoveries
f) Department/Branch/ Business Unit
g) Actions taken since the occurrence

5.0 Roles and Responsibilities

All staff are involved in the management of operational risk within the Bank. Hence it is the responsibility of all staff to provide information on loss events that occur. However, the following officers are directly and specifically responsible for reporting losses:

5.1 OpRisk Champions (ORCs):

1) Reporting all loss events from the activities going on in any Unit/Department/Branch shall be the responsibility of the respective OpRisk Champion. The Service Managers are designated ORCs in their respective branches.

2) The ORCs must ensure that cost of replacing damaged assets (ranging from office equipment to pool vehicles and physical structures), fraud issues (both internal and external), litigations against the Bank, reversals from the P&L, robberies, burglaries etc. are reported and recorded in the loss database kept by ORM

3) Additional information/reports shall be required from specific units/departments to ensure the completeness of the loss capturing process.

4) The OpRisk Champion for Legal shall ensure that all costs associated with litigations filed against the Bank are reported as they occur. Additional information/reports will be detailed The report will be detailed to differentiate the various costs involved as ‘well as the amount claimed by the claimant.

5.2 Control & Assurance Function

Head, Internal Audit or CAE shall on a monthly basis report fraud, forgeries and other loss related information to the Head Operational Risk Management.

5.3 Operational Risk Management

The classification of all the loss reports into the Basel loss event types shall be the sole responsibility of Operational Risk Management.

6.0 Other Issues

Indemnity shall be provided against disciplinary proceedings to those who caused and reported events, except in instances of criminal activity or gross policy violations. Confidentiality of those involved shall be maintained. The reporting should not reveal the identity of any employees involved.

7.0 Amendment and Exceptions

Periodically, there may be a need to amend or deviate from this policy due to either government regulations or other circumstances. Any amendment\exceptions must receive the appropriate referencing to the existing document. Amendments/exceptions must receive the appropriate approval. All exceptions to this policy must also be documented and tracked by Operational Risk Management.

8.0 Policy Review

This policy shall be reviewed every three years or on a more frequent basis if deemed necessary.

Appendix I: Loss Definitions

a. **Actual loss**: This refers to the loss value before recoveries of any type.

b. **Net loss**: This shall be taken as the loss after taking into consideration the impact of recovery.

c. **Near miss**: This is an unplanned event (that has occurred) which has the potential for causing any form of financial loss to the Bank but does not due to a fortunate break in the chain of events. Events like this must be captured for the purpose of improving our control points.

d. **Potential loss**: This refers to incidents that have occurred but the impact is yet to be fully determined. These events are such that they may or may not lead to some form of financial loss to the Bank.

Appendix II: Basel Event Classification

Basel II loss event categorization for operational risk loss data base management

A loss is recognised as an operational loss if it is not a credit loss and it occurred as a result of any of the seven event types for operational risks. These include:

Basel Event Classification				
S/No	**Event Type Level 1**	**Event Type Level 2**	**Event Type Level 3**	**Description**
1	**Internal Fraud** *these are losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.*	**Unauthorized activities**	**Intentional suppression of transactions**	This is a situation where a staff intentionally fails to record transactions or records only a part of the transaction
			Intentional mismarking of position	This is a situation where some of the Bank's assets or liabilities are intentionally revalued using wrong market indices to create false impression of a gain.
			Unauthorized Transaction	This occurs when the Bank's employee enters into transactions that are outside the sphere of the Bank's business or transactions that the employee is not empowered to carry out. For example approving a transaction outside authority/approval limit.
		Theft and Fraud	**Fraud and Forgery**	This refers to intentional acts which may involve the falsification of documents and records and the misappropriation of assets.
			Worthless Deposit	Intentional presentation of cheques through clearing when there is insufficient credit in the drawer's account.

			Extortion	This occurs when staffs of the Bank use his/her official position to illegally obtain property, funds or patronage from the Bank or from his/her subordinate by coercion or intimidation.
			Embezzlement	This describes instances where an employee diverts the Banks' funds for personal use.
			Robbery	This occurs when a bank staff (by way of providing critical information) in conjunction with a third party attacks the Bank and carts away money and other valuables.
			Misappropriation of Assets	Illegal conversion of bank's properties to personal ownership.
			Account take-over	These are instances where a staff having information about the inability of a customer to continue running his/her account as a result of infirmity, death or indictment for crime etc. takes over such an account and carries out normal banking activities on that account.
			Impersonation	This occurs when a staff fraudulently assumes the appearance of another staff (not necessarily a superior officer) of the Bank or of a customer for personal gains.
			Insider Trading	This occurs when an employee uses information at his disposal as a result of his office or position to affect his personal business decisions for his own benefit.
			Bribes and Kick-backs	This describes situations where staff of the Bank uses his/her official position to illegally favor a staff or a customer as a result of some kind of benefit to be derived from such favors.

2.	**External Fraud** *these are losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a party external to the Bank.*	**Systems security**	**Systems Hacking.**	This explains situations where third parties with the aid of IT related equipment, processes and procedures breaks into the Bank's network or system
			Theft of Information resulting in monetary loss	This explains situations where vital information are stolen by third parties and then used to obtain fraudulent monetary gratification or uses such information to blackmail the Bank leading to loss of monetary values.
		Theft and Fraud	**Theft/Robbery**	This represents situations where persons other than employees of the Bank cart away the Bank's property, money and other valuables without the help of insider information
			Fraud and Forgery	This represents instances when a person other than a bank staff deliberately engages in acts intended to deceive the Bank with the aim of personal enrichment.
			Cheque Kiting	This describes situations where a customer having accounts with several banks uses cheques to move an amount of money round the Banks making it look as if there were actual movement of funds.
3.	**Employment practices & work place safety.**	**Diversity and discrimination**	**Discrimination of all types**	This represents instances where staff is maltreated for no reason other than tribal, sexual or religious differences.

	these are losses arising from an act inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.	**Employee Relations**	**Compensation**	Inadequate compensation/money given or received as payment or reparation for service or loss
			Benefit	Disruption of business activities arising from deficient conditions of employment or refusal to implement the terms and conditions of employment with regard to entitlement or provision for health insurance policy, holiday allowance, etc.
			Termination Issues	Disruption in normal banking transactions as a result of disagreement over the way and manner the contract of employment of an employee is terminated.
			Organized labor activity	Business disruption as a result of issues emanating from the activities of the organized labor and trade unions.
		Safe Environment	**Workers compensation**	Situations of inadequate compensation or payment for loss suffered in the course of the lawful discharge of duty
			Employee health and safety rules events.	Lack of or inadequate provision in the health and safety rules resulting in personal loss to staff e.g. lack of first aid treatment to give primary medical attention to an employee who got injured in the course of service leading to his death or disability.
			General Liability	Instances where the Bank is held legally responsible for some injury or damage (which may have led to financial losses for the Bank) as a result of inadequate insurance policy to cover such losses.
4	**Damage to Physical Properties.** *the loss or damage to physical assets from*	**Disasters and other events**	**Losses from natural disaster**	This covers Instances of losses or destruction to Bank's properties and assets as a result of natural disaster.
			Human losses from external sources	Loss of the Bank's properties as a result of human activities.

	natural disaster or other events.			
5.	**Business disruption & system failure.** *these are losses due to disruption of business or system failures.*	**Systems**	**Hardware failures**	Situations where there are disruptions of business activities as a result of the inability of the physical parts or component of the computer to function within specified performance requirements or thresholds.
			Software failures	Situations where there are disruptions of business activities as a result of the inability of the nonphysical parts or component of the computer to perform its required functions within specified performance requirements or thresholds.
			Telecommunication failures	Business failures arising from breakdown of telecommunication systems such as telegraph, cable, telephone, radio etc.
			Utility Outage	Business disruption arising from power outages from NEPA, water outages and other utility outages.
			Network failure	The total time the system is out of service due to hardware/software failure, scheduled maintenance, malfunction or natural / human-caused disaster.
			Generator Breakdown.	Disruption in banking transactions as a result of generator breakdown.
			Other forms of disruption.	All other forms of business disruption caused by factors not mentioned above.
			Unrest, riots, curfews,	Losses and situations arising as a result of civil unrest, curfews, activities of area boys and touts etc.
6.	**Clients, Products & Business Practices**	**Suitability, Disclosure and Fiduciary**	**Fiduciary breaches / guidelines violations**	Losses arising from situations where the Bank failed in its duties of trust to customers.
			Disclosure issues	Issues relating to implementation of KYC

	these are losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.		**Breach of privacy**	Situations of unnecessary interference in private information of a customer.
			Retail customer disclosure violations	Divulging customer's business information entrust to the Bank's staff in the normal course of business which can result in a claim on the Bank e.g. divulging a customer's a/c balance to unauthorized persons.
			Account churning	This captures information on the rate of closure of accounts by customers of the Bank as a result of dissatisfaction with the Bank's service.
			Misuse of confidential information	Instances where certain customer information is used wrongly.
		Improper business or market practices.	**Anti-trust**	This describes situations where the Bank engages in activities that stifle competition and creates a situation of monopoly in the industry.
			Improper trade practices	This describes situations where the Bank engages in unethical practices.
			Unlicensed activities.	Losses arising from the Bank engaging in unlicensed activities.
			Money laundering	All money laundering related issues.
		Product flaws	**Product defect**	This deals with instances where the Bank's product fail to meet required advertised standards leading to loss of public patronage on that product
		Advisory Activities	**Disputes over performance of advisory service**	Business disruption / losses arising from providing advisory services to customers of the Bank.
7	**Execution, Delivery & Process Mgt.**	**Transaction capture, execution & maintenance**	**Data entry maintenance or loading error**	Instances of wrong capturing of data. Example will include error made when the Bank credits a group of customers with their monthly salaries as a result of the Bank acting as a paying bank to the customers' employer.

	these are losses arising from failed transaction processing or process management, from relations with trade counterparties and vendors.		**Missed deadline or responsibility**	Instances where the Bank fails to meet customer's transactions or regulatory deadlines.
			System malfunctions.	This describes all instances where system output is at variance with expected output.
			Accounting error	Errors arising from applying the wrong accounting treatment to transactions.
			Entity attribution error	This situation occurs when an account or customer file is erroneously updated with information meant for another account or customer file as a result of similarity in the account number or customer name
			Other task mis- performance	This describes other forms of mis-performance of task not described above.
			Delivery failure	When the Bank fails to meet a contractual agreement that has to do with delivery of documents, cash etc.
			Collateral management failure	Situations where the Bank's staff compromise standards in the management of collaterals used as security for credit and when such credits go bad this collateral could no longer mitigate the Bank's losses
		Monitoring & Reporting	**Failed mandatory reporting obligation**	Instances where the Bank fails to render returns or certain reports as may be required by the regulatory authorities from time to time
		Customer Intake and Documentation	**Legal documents (missing or incomplete)**	Situation where certain statutory legal documents relating to certain transaction or customers are misplaced or were not well articulated at the point of going into contractual agreement.
		Customer/Client Account Mgt.	**Unapproved access given to accounts**	Situations where access is given to accounts that ideally should not be given access as a result of incomplete documentation.

			Incorrect client records	Situations arising from instances where the Bank fails to capture correct client or customer information.
			Negligent loss or damage of client assets	Describes instances of loss of client or customer property in possession of the Bank.
		Trade C/P	**Misc. c/p disputes**	All other social or business dispute between the Bank and non-customers.
		Vendors and	**Outsourcing**	Business disruptions arising from contracts entered into with other persons or companies to offer technical or other services to the Bank.
		Supplies	**Vendor disputes**	Instances where there are disputes with suppliers of equipment to the Bank.

Appendix III: Costs to be Included & Excluded in estimating OR Loss Amount

Costs to be Included & Excluded				
S/No	**Costs Category**	**Definition / Discussion**	**Examples of loss effects**	**Reporting requirement**
1	**Legal** *Does the loss result from a legal dispute?*	**Judgements, settlements and other legal costs.**	Costs incurred in connection with litigation in a court proceeding or arbitration (including external attorneys' fees, settlements, judgements paid, etc.)	Included
			External Legal costs directly associated with event	Included
			Write-down based on G.A.A.P.	Included
			External Legal costs related to improvements in documentation / processing	Excluded
2	**Restitution** *Does the loss involve payments to third parties?*	**Payments to third parties on account of operational losses for which the bank is legally responsible.**	Claim from client due to business interruption loss (for which Bank is responsible)	Included
			Pricing error results in claim from client for compensation by the bank	Included
			Net interest cost due to delays in settlement	Included

			Confidential client information lost in burglary, client suffers loss and claims against bank	Included
			Employee fraud results in bank replacing lost client funds/assets	Included
			External fraud results in loss of client funds requiring the bank to make a payment to the client to compensate the loss	Included
			Reduction in bank's own revenues due to business interruption (opportunity costs not included)	Excluded
			External security breach results in reputation damage	Excluded
			Reimburse client for loss to preserve relationship, goodwill payments	Excluded
3	**Loss of Recourse** *Does the loss result from a bank's inability to enforce its claims on third parties, other than credit*	**Losses experienced when a third party does not meet its obligations to the bank, and which are attributable to an operational mistake or event**	Funds transferred by mistake to incorrect counterparties or duplicate payments made, unable to be recovered.	Included
			Credit-related operational loss: loan documentation errors, monitoring inadequacies, failure to perfect security interest	Included
			Inability to enforce netting agreement due to inadequacies in documentation or failure to verify counterparty	Included
			Losses in interest income as result of not changing the interest rate due to human error	Included
			Anything recorded purely as "credit risk" without any operational loss element under final Basle Accord. View separate paragraph on operational losses in credit risk incidents	Excluded
			Loss after implementing netting agreement in bankruptcy (credit risk)	Excluded
4	**Regulatory Action**	**Represents fines or any direct payment of any penalties incurred as a result of**	Fines / Penalties paid to regulatory agencies,	Included
			Fines / Penalties paid to the government	Included
			Attorney fees paid for representing the bank at hearing on regulatory violation	Included

		the operational risk loss event	Loss of revenue due to license revocation, Attorney fees paid in testifying before regulators, seeking change in a regulatory provision that would favour the Bank	Excluded
5	**Loss or Damage to Assets**	**Represents direct reduction in the value of physical assets due to some kind of accident (e.g. neglect, accident fire and natural disasters,**	Cost to re-locate short term, business continuity,	Included
			Use of third party supplier to continue business	Included
			Costs associated with making the premises fit for business after fire, flood or other natural disasters	Included
			Write-downs / write-offs (net book value) of assets due to fire, flood or other natural disaster	Included
			Loss / destruction of intangible property (e.g. data)	Included
			Improvements made in the course of repairs of premises after fire, flood or other natural disasters	Excluded
6	**Other write-off**	**Direct reduction in the value of assets due to theft, fraud, unauthorized activity or market or credit losses arising as a result of operational events.**	Failure to deliver / acquire asset in time and market price moves	Included
			Losses from unauthorized trade (“rogue trading”)	Included
			Loss from trades in excess of established market exposure limits	Included
			Pricing error results in lower-than-expected revenue	Included
			Employee fraud results in bank writing-off the loss	Included
			External fraud or theft results in loss of bank assets/revenues	Included
			External security breach results in hiring of consultants to determine nature of problem and fix it	Included
			Market risk loss due to system or human error or due to (internal) fraud	Included
			Anything recorded purely as a “market risk loss” without an operational loss element under final Basle Accord	Excluded
7	**Miscellaneous**		Costs related to consultants / third parties to investigate/fix (may be in various categories)	Included
			Costs associated with failed outsourcing assignment (may be in various categories)	Included

			Control breakdown that leads to an operational loss, requiring consultants to understand the cause of the problem and propose remedies.	Included
			Management time to fix/investigate the event	Excluded
			Costs of internal support department (part of regular work activity) to investigate/fix (e.g., Audit, IT support)	Excluded
			System upgrade costs included in fixing a problem	Excluded
			Improvement in compliance/controls to prevent recurrence of problem	Excluded
			Purchase of new equipment due to failure of old equipment	Excluded
			Cost to replace staff	Excluded
			Reduction in revenues due to loss in key staff (business risk)	Excluded
			Reduction in revenue due to damage to reputation	Excluded
			Control breakdown that does not lead to a loss, but requires hiring resources (e.g., consultants)	Excluded

APPROVAL DETAILS & VERSION CONTROL		SIGNATURE
DOCUMENT NAME	LOSS DATA MANAGEMENT POLICY	
OWNER	OPERATIONAL RISK MANAGEMENT	
AUTHOR	HEAD, OPERATIONAL RISK MANAGEMENT	
REVIEWER	CHIEF RISK OFFICER	
FINAL APPROVAL	RISK MANAGEMENT COMMITTEE	
VERSION	VERSION 1	
DATE OF APPROVAL	DECEMBER 21, 2022	