PARAMOUNT LIFE & GENERAL INSURANCE CORPORATION

RISK MANAGEMENT STRATEGY

1. INTRODUCTION

1.1 . POLICY STATEMENT

PARAMOUNT LIFE AND GENERAL INSURANCE CORPORATION ("Company") is in the business of managing risk. The Company's ability to satisfy customers' risk management needs is central to what the Company does. The Company aims to generate wealth and maximize returns for its shareholders by pursuing opportunities that involve risk. The Company's people have the responsibility to ensure that the key risks are managed and controlled on a day-to-day basis. The Company aims to use its ability to properly manage risk to provide more certainty and improved outcomes for all stakeholders.

The Company seeks to only take on risks that fall within the Company's stated risk appetite and aims to manage them in a way to achieve an optimal return overall. The Company's ERM Framework is designed to support this approach and enhance decision-making by its people. A strong approach to risk management informs decision-making and enables the Company to measure and judge its risk exposures. Ultimately, this gives the Company greater confidence and expands its capacity to take on risks to improve returns.

The Company defines a risk event as an incident or occurrence that could happen, or has already happened and impacts on the achievement of its objectives or performance.

1.2. PURPOSE

This Risk Management Strategy (RMS) outlines the Company's strategy for managing risk and the key elements of the Company's ERM Framework that give effect to this strategy. This includes risk appetite, the governance arrangements and key roles and responsibilities relating to risk management and the key risk processes and reporting mechanisms used within the Company to manage risk.

1.3. SCOPE

The Company must ensure that systems and controls are in place to ensure adherence to the Company's roles and responsibilities set out in this Policy and compliance with regulatory requirements. In any cases where new regulatory requirements materially conflict with this strategy, the new requirements must be complied with; and the CEO, President, and CRO must be notified of any material deviations from the strategy.

2. RISK MANAGEMENT FRAMEWORK

2.1. OVERVIEW

The Company's ERM Framework includes the following key components:

- ***risk categories*** – the key risk types that the Company is exposed to;
- ***risk appetite*** – the level of risk that the Board and management are prepared to take in pursuit of the organization's objectives. Risk appetite is linked to business strategy;
- ***governance*** – establishes authority, accountability and responsibilities in relation to risk and management. The Company's risk governance model reflects a "three lines of defence" approach. Other key components of the Company's broader governance framework include policy governance, delegations of authority, culture and training. The risk governance framework is linked to the corporate governance framework;
- ***reporting*** – risk information flows through the governance framework to ensure that there is appropriate management of risk and exposures are in line with the defined risk appetite;
- ***risk management processes*** – includes Risk and Control Assessment (RCA), Divisional Risk Assessment (DRA), Total Risk Assessment (TRA), control assurance, targeted risk reviews, Key Risk Indicators (KRIs), Internal Loss Events (ILE) and stress testing and scenario analysis;
- ***risk data / management information*** – collected and collated through various risk management processes. This is used as input to risk models and for reporting through the governance framework;
- ***issues and actions*** – management activity required to resolve problems or address improvements identified through the risk processes or otherwise;
- ***risk culture*** – observable patterns of behavior in the way employees perform their work, as it relates to risk management, and the judgements they make; and

The Company will implement all components of the ERM Framework. However, this is subject to risk and compliance plan and resource availability.

2.2. RISK MANAGEMENT APPROACH

As noted in section 1.3, this RMS outlines the Company's strategy for managing risk and the key elements of the ERM Framework that give effect to this strategy.

The Company's strategy for managing risk is to:

- achieve competitive advantage by better understanding the risk environments in which we operate;
- operate within our stated risk appetite and more effectively allocate capital and resources by assessing the balance of risk and reward; and
- avoid unwelcome surprises by reducing uncertainty and volatility through the identification and management of risks to the achievement of business objectives.

The Company aims to adopt a rigorous approach to managing risk throughout the Company. The key objectives of the Company's approach to risk management are to:

- drive conscious and objective risk-based decisions to optimize return;
- give confidence to the business to actively take appropriate risks; and
- adopt leading practices and a single ERM approach globally that allows for more consistent and improved outcomes.

2.3. RISK CATEGORIES

The Company identifies and assesses the risks to delivering on its strategic and business objectives. These risks are then categorized into one of seven categories for aggregation, reporting and modelling purposes. The seven categories are as follows:

- **Strategic Risk** – the current and prospective impact on earnings and or capital arising from strategic business decisions and responsiveness to external change. Includes the following sub categories:
    - business product, market, and distribution approach;
    - capital structure and management;
    - acquisition decision and negotiation;
    - tax planning and decisioning; and
    - investment strategy.

- **Insurance Risk** – the risk of fluctuations in the timing, frequency and severity of insured events and claims settlements, relative to expectations. Includes the following sub categories:
    - underwriting/pricing;
    - insurance concentrations;
    - reserving; and
    - reinsurance.

- **Financial Risk** – the risk of variation in the value of investments due to movements in market factors. Market factors include but are not limited to: interest rates, credit spreads, foreign exchange rates, equity prices and commodity derivatives. Includes the following sub categories:
    - investment market movement (including equity, interest rate, credit spreads);
    - foreign exchange rate movement.

The risk of insufficient liquid assets to meet liabilities as they fall due to policyholders and creditors or only being able to do so at excessive cost.

- **Operational Risk** – the risk of financial loss resulting from inadequate or failed internal processes, people and systems or from external events. Includes the following sub categories:
    - internal fraud;
    - external fraud;
    - employment practices (people risks);
    - improper business practices;
    - disasters and other events;
    - technology and infrastructure failures; and
    - business and transaction processing.

2.4. MANAGEMENT OF KEY RISKS

Given the changing nature of the environment in which the Company operates, it is imperative that the Company's risk management continues to evolve and adapt. The Company identifies risks to achieving our business objectives, takes a forward-looking approach to managing risk and continually monitors its exposures against stated risk appetites.

The Company has established internal systems and controls to manage material business risks in the key areas of exposure relevant to the Company. These internal systems and controls are designed to provide reasonable assurance that the assets and revenues of the Company are safeguarded and that exposures remain within stated risk appetites.

The following table provides some examples of the key drivers for each risk category and key risk mitigation approaches.

Risk Category	Key Drivers	Key Mitigation Approaches
Strategic Risk	▪ Changes in the external environment including competitive landscape, customer behaviour and distribution models ▪ Business strategy and change, investment strategy, tax strategy and corporate governance ▪ Risks related to acquisitions and capital management	▪ Defined strategic risk appetite ▪ Considering strategic options in light of the impact on return volatility and capital requirements ▪ Scenario planning augmented by use of an economic capital model (ECM) in assessing capital requirements and allocation for insurance, credit, market, liquidity, operational and group risk ▪ Planning and monitoring capital levels on an ongoing basis, with reference to regulatory and rating agency requirements and other benchmarks ▪ Assessing acquisition strategic fit and setting minimum requirements for conducting due diligence

Risk Category	Key Drivers	Key Mitigation Approaches
Insurance Risk	▪ Pricing and underwriting of individual insurance contracts ▪ Uncertainty around insurance relating to the timing and size of insurance claims reporting and settlement ▪ Accumulations of underwriting exposures to both catastrophic and gradual claims ▪ Effectiveness of the purchased reinsurance programme	▪ Defined insurance risk appetite ▪ Underwriting strategy and delegated authorities ▪ Use of pricing models and monitoring of rate changes on renewal ▪ Business planning processes ▪ Modelling including catastrophe models and the ECM ▪ Monitoring underwriting risk aggregations ▪ In-house and external actuarial review of claims provisions independent of underwriting teams ▪ Reinsurance purchase monitoring

Risk Category	Key Drivers	Key Mitigation Approaches
Financial Risk	▪ Market dynamics ▪ Change in market value and/or volatility of portfolios ▪ Changes in interest rates or shape of yield curve ▪ Changes in spot/forward currency rates, volatility and correlations. ▪ Cash inflows from premiums, investment income, capital injections, dividends and loans ▪ Cash outflows for claims and redemptions, debt service requirements, tax payments, dividends and expenses ▪ Cash collateral requirements	▪ Defined market risk appetite ▪ Defined Market Risk Management Strategy ▪ Independent oversight of market risk ▪ Defined liquidity risk appetite ▪ Holding a minimum percentage of liabilities in liquid assets ▪ Maintaining sufficient liquidity in investment portfolios to address claims needs ▪ Cash flow targeting ▪ Cash flow forecasting ▪ Stress testing of liquidity needs relative to major catastrophe events ▪ Contingency planning ▪ Negotiating cash call clauses in reinsurance contracts and seeking accelerated settlements for large reinsurance recoveries ▪ Banking facilities ▪ Asset/liability matching of major currency holdings and claims payment patterns

Risk Category	Key Drivers	Key Mitigation Approaches
Operational Risk	▪ Process complexity ▪ Ageing or non-integrated systems ▪ Capability, experience and training of employees ▪ Environmental or other external factors	▪ Defined operational risk appetite ▪ Active monitoring of key processes ▪ Scenario reviews to identify and quantify potential exposures for mitigation ▪ Effective segregation of duties, access controls, authorisation and reconciliation procedures ▪ Business continuity management and disaster recovery planning and testing ▪ Information security management ▪ Physical security management

2.5. EMERGING RISKS

The Company defines emerging risks as new risks characterised by incomplete but developing knowledge or existing risks that develop in novel or unexpected ways. To be considered “emerging” there must be:

- some *uncertainty* around the understanding of the risk, that is, uncertainty as to its emergence at all or as to the timing and impact in operational and financial terms; and
- some evidence to support the potential for the risk occurring, that is, it must be *realistic*; and
- potential for *material* impact to the Company's business from a financial and / or operational perspective.

A risk is no longer "emerging" when the risk is managed as "business as usual" or there is an ability to quantify, with some confidence, the likelihood of the occurrence and the impact in operational and financial terms.

The Company monitors emerging risks and their potential impact on the Company through the following activities:

- regular review of existing identified emerging risks;
- assessing potential impact;
- identifying new emerging risks (horizon scanning);
- raising awareness of emerging risks across the Company;
- undertaking research on specific emerging risks; and
- developing recommendations for consideration by Board, and senior management as appropriate

3. RISK APPETITE

Risk Appetite is the level of risk that the Board and management are prepared to take in pursuit of the Company's objectives. The Company's risk appetite process aims to ensure consistency in how risk appetite is defined, communicated, monitored and reported, and outlines how risk appetite statements are cascaded and applied within the Company.

Risk appetite is formally reviewed by the Board to ensure that business strategy and risk appetite are aligned. Risk appetite is also reviewed throughout the year to reflect changes to strategic objectives or significant changes to the internal or external business environment. Following approval by the Board, risk appetite statements form the starting point for the Company risk appetite statements.

There are three key aspects to the risk appetite process, as follows:

- setting / articulation – risk appetite is defined in accordance with an established risk appetite hierarchy that outlines how risk appetite statements are structured and is articulated in accordance with defined principles. Statements are established and must be set, reviewed and approved by the Board;
- communication – the risk appetite owner is responsible for determining how the statement(s) should be communicated across the Company and is also expected to identify the required audience, what will be communicated and the method of communication for each group. Expectations around risk appetite should also be clearly communicated, especially for those with a specific role in the process. General awareness of risk appetite should be achieved through both ERM and more general training; and

- monitoring and reporting –monitoring is conducted in accordance with the frequencies defined in the risk appetite setting stage. Breaches should be escalated and actions implemented to address breaches in accordance with the issues and actions process. Regular reporting to the Board and Risk Management Committee is undertaken in accordance with prescribed pro-forma and all breaches should be reported together with details of actions to address.

4. GOVERNANCE

4.1. RISK GOVERNANCE

Within the context of the Company's corporate governance framework, the Company has a defined risk governance framework that is designed to clearly establish authority, accountability and responsibilities in relation to risk management and aims to ensure that the ERM Framework and processes are robust and appropriate.

The Company's risk governance framework reflects the three lines of defense approach to risk management. This defines risk management responsibilities across the Company.

The first line is responsible for implementing the ERM Framework and associated policies and procedures to manage the risks inherent in their business. The second line is responsible for developing the framework and processes used by the first line to manage risk and for monitoring the quality and effectiveness of implementation of these processes. The third line of defense is responsible for providing independent assurance over the first and second lines' delivery of their responsibilities and the adequacy of the internal control environment.

4.1.1. Oversight

- **Board of Directors**

The Board monitors the performance of the Company and as such fulfils a critical role in ensuring that an effective RMS is established and maintained. The Board is responsible for overseeing the Company's ERM Framework and at least annually, approves the Risk Appetite Statements, RMS and Business Plan.

- **Risk Management Committee (RMC)**

The Risk Management Committee's role is to assist the Board in overseeing the design and implementation of the Company's ERM Framework together with the capital requirements of the Company. In relation to the Company's risks, the RMC considers the process of risk identification, assessment and management actions; material risks, including emerging risks; risk appetite; key risk policies and risk management reporting.

- **Audit Committee (AC)**

The AC's role is to assist the Board in overseeing the integrity of the financial reporting process of the Company, including the scope and outcome of external and internal audits.

4.1.2. First Line of Defense

Risk Ownership

Business units (departments) generate most of the risk exposures and have responsibility for identifying, controlling and owning risks. Each key risk applicable to the business unit (department) is assigned a risk owner; the individual with accountability and authority for managing the risk. However, it is the responsibility of every employee to adopt a rigorous approach to managing risks.

4.1.3. Second Line of Defense

Risk and Compliance Officer

The role and function of the Risk and Compliance Officer among others is to:

- Supervises the entire ERM process and spearheads the development, implementation, maintenance and continuous improvement of ERM processes and documentation;

- Communicates the top risks and the status of implementation of risk management strategies and action plans to the Risk Management Committee;

- Collaborates with the CEO in updating and making recommendations to the Risk Management Committee;

- Suggests ERM policies and related guidance, as may be needed; and

- Provides insights on the following: Risk management processes are performing as intended; Risk measures reported are continuously reviewed by risk owners for effectiveness; and Established risk policies and procedures are being complied with.

There should be clear communication between the Risk Management Committee and the Risk and Compliance Officer.

Actuarial Review

The Company's outstanding claims provision is reviewed by experienced actuarial staff. Actuarial staff are involved in forming an independent view, separate from management, of the central estimate and the probability of adequacy of the outstanding claims provision and premium liabilities.

4.1.4. Third Line of Defense

Internal Audit

The Company appoints the Internal Audit (IA) unit, which is headed by the Head of Internal Audit and reports to the Board. As the third line of defense, it is independent and objective, having no direct authority or responsibility for the activities it reviews. The primary role of IA is to assist the Board of Directors and senior management in the discharge of their responsibilities for the sound and prudent management of the Company.

IA operates under a written Internal Audit Charter that is formally approved by the Board. The Charter establishes the authority, independence and responsibilities of IA and defines the purpose, role, authority, organization, independence, scope, audit planning, reporting, quality assurance and periodic assessment of the internal audit function within the Company. The scope of internal audit, including its Charter, is regularly reviewed by the Board.

IA operates within an established framework designed to meet stakeholder expectations and achieve adherence to applicable technical and professional guidelines and regulations including the Institute of Internal Auditors' 'Code of Ethics' and the Institute's 'International Standards for the Professional

Practice of Internal Auditing' (Standards) and other applicable technical and professional guidelines and regulations.

External Audit

The external audit is conducted under a letter of engagement approved by the Board. The external auditors are required to issue an audit opinion on the annual financial statements of the Company's financial statements in accordance with regulatory standards.

The external auditors are required to produce an annual report to the Insurance Commission of the Philippines (IC). The external auditors must also conduct a limited assurance review in respect of the Company's compliance with all prudential requirements (including risk and reinsurance management).

4.2. Delegation of Authority

The Company operates under an extensive system of delegated authorities. Delegated authorities are a key component of the Company's governance and risk management frameworks. Delegated authorities:

- support the achievement of the Company's strategy and supporting business plans;
- support the structured, measured and consistent cascade of risk appetite set by the Board;
- appropriately empower employees to make decisions and complete transactions within clearly defined risk limits; and
- control the extent to which employees can commit the Company.

The mechanism for delegating authority throughout the Company is as follows:

- authority is delegated by the Board to the CEO and President;
- authority is delegated by the CEO and President to senior management and all relevant employees across the Company.

Compliance with delegated authorities is monitored. This further reinforces ownership of, and accountability for, risk management throughout the Company.

4.3. Training

The Company has appropriate ERM training programs in place to support the implementation and embedding of the ERM Framework. The ERM training:

- assists individuals in their understanding of their responsibilities and the Company's risk appetites;
- supports and promotes a positive risk and control culture;
- supports better business decision-making; and
- supports the integration of risk management into the broader management processes of the Company.

The Company's training approach is comprised of the following key steps:

- audience categorization – to determine the level of risk training and to allow for tailoring of training content and delivery;
- identification of knowledge requirements – allocation of the identified audience to the appropriate level of training via a knowledge matrix;
- determination of delivery method – a variety of delivery methods can be used to suit the needs of each audience category and knowledge level;
- development of training material – will depend on the audience, knowledge requirements and delivery method; and
- delivery of training – in line with the above.

5. REPORTING

The Company's governance framework is supported by risk reporting, which is used to provide complete, accurate and timely risk data and analysis that can be used to support day-to-day business decisions.

Key stakeholders for risk reporting include boards, committees, risk owners, business management and support functions. In particular, risk and performance-related information is routinely reported to the Board and Risk Management Committee. Some of the key risk data reported includes:

- updates on key risk activities;
- adherence to risk appetite,
- key risks and the assessments of these risks;
- assessment of control frameworks;
- ILEs (number of events and impacts);
- Issues (details of critical and high rated, proportion self-reported, proportion overdue and revised due dates);
- IA reports to the AC (including the annual review of the ERM Framework); and
- external audit reports.

6. RISK MANAGEMENT PROCESS

6.1. Overview

The Company's risk management processes comprise a number of key elements, as follows:

- **Risk and Control Assessment (RCA)** – to identify and assess the key risks that the Company faces in delivering on its strategic and business objectives over a 12-month horizon and to assess the effectiveness of the controls in place to manage these risks;

- **Control Assurance** – ongoing assessment and testing of key controls' design and performance;
- **Key Risk Indicators (KRIs)** – provide a current and trending view on levels of exposure to particular risks;
- **Internal Loss Events (ILE)** – to assist the business in identifying and quantifying ILEs, support management of ILEs and create a process for the escalation of ILEs to alert management to areas where action is required.

6.2. Risk and Control Assessment (RCA)

The RCA process enables the Company to identify and assess the key risks that it faces at a business unit level in delivering on its strategic and business objectives over a 12-month horizon and assess the effectiveness of the controls in place to manage these risks. The Company uses the RCA process to identify and assess risks and controls across all risk categories.

The assessment stage includes the following key components:

- **Control Assessment**

The controls relating to each risk are collectively assessed based on design and performance in accordance with the tables below. This assesses the combined design and the combined performance of the controls in mitigating the risk. The Company may choose to individually assess each control using the same tables.

- **Control Design**

Evaluation	Guidance
Adequate	Control design is reliable in mitigating the risk(s) as required.
Partially Adequate	Control design is reliable in most cases; however, marginal improvement is needed to mitigate the risk(s) as required.
Not Adequate	Design of the control is unreliable; control design requires substantial improvement to mitigate the risk(s) as required.

- **Control Performance**

Evaluation	Guidance
Effective	Control performance is reliable in mitigating the risk(s) as required.
Partially Effective	Control performance is reliable in most cases; however, marginal improvement is needed to mitigate the risk(s) as required.
Not Effective	Performance of the control is unreliable; control performance requires substantial improvement to mitigate the risk(s) as required.

- **Overall Control Effectiveness**

Evaluation	Guidance
Effective	Overall, the design and performance of related controls are reliable in mitigating the risk as required.
Substantially Effective	Overall, the design and performance of related controls are reliable in most cases; however marginal improvement is needed to mitigate the risk as required.
Partially Effective	Overall, the design and performance of related controls are reliable only in limited circumstances and require a marked improvement to mitigate the risk as required.
Not Effective	Overall, the design and performance of related controls are unreliable in mitigating the risk as required.

- **Residual Risk Assessment**

Residual risk is the exposure to a risk having considered the overall control effectiveness.

Operational risks are assessed based on frequency and severity as follows:

- **Frequency Assessment**

Frequency is defined as “the estimated number of risk events in the next 12 months”.

- **Severity Assessment**

Severity is assessed using both the financial and non-financial impact. Financial severity is defined as the “estimated typical loss per event” and is assessed on a median or “middle-o-the-range” gross loss basis.

Non-financial severity is considered based on four factors: reputational impact; regulatory impact; staff health and safety; and business disruption and management effort. Opportunity costs may be included in the Non-financial Severity Assessment under Reputational impact.

A four-level rating scale applies to each of these factors, as illustrated in the table below:

Impact	Low	Medium	High	Critical
Reputational Impact	Complaints from a relatively small number of stakeholders with no media coverage	Complaints from a small number of stakeholders and/or limited adverse local / state media coverage	A noticeable increase in the volume of stakeholder complaints and/or short- term adverse national or international media coverage	Significant number of stakeholder complaints and/or extended adverse national and or international media coverage
Regulatory Impact	Cautioned or repeatedly cautioned by regulator for minor breaches	Escalation in supervision by regulator resulting in increased reporting requirements	Adverse directive issued by regulator to senior management or board	Sanction from regulator
Staff health and safety	Loss of a staff member from work through injury or illness	Loss of multiple staff members from work through injury or illness	Major injury to staff as a result of a workplace health and safety or potential for short-term wide-spread impact on staff	Potential / actual death of staff member(s) or potential for wide-spread impact on staff health or safety
Business disruptions and management effort	Some disruption which can be absorbed through normal management activities	Reprioritisation of management activities required and senior management required for decision-making	Reprioritisation of management activities required and President & CEO required for decision-making	Redirection of management activities and staff to address the issue. Support (external or otherwise) is required to maintain BAU activities

- **Risk Response**

Risk Response	Guidance
No Action Required	No key actions are required to manage this risk
Monitor Risk	The risk should be regularly monitored to ensure that it remains stable
Action Required	Actions should be taken in the short to medium term to either improve controls or prevent the risk from breaching appetite
Immediate Action Required	Actions should be taken immediately to either improve controls, bring the risk back within appetite or prevent it from breaching appetite

Once the risk assessments are complete, the risk owner determines the appropriate response to the risk. The Company uses four response categories, as detailed in the table below. When determining the risk response, the risk assessment and risk appetite should be considered, i.e. if not within appetite, the response should be ‘immediate action required’.

6.3. Control Assurance

The first line undertakes regular testing of their operational controls. The results of this testing are reflected in RCAs and audit reviews.

Assurance over the effectiveness of controls is provided in a number of ways. A key mechanism is the ongoing monitoring by the first line of defense as part of day-to-day activities. Management refer to a number of sources of information including, but not limited to, KRIs, key performance indicators, Quality Assurance reviews, technical audits, ILEs, issues and actions and other management information.

In addition to ongoing control monitoring, further assurance can be gained through control testing. Control testing may be conducted by any of the three lines of defense and involves various approaches, with the most suitable approach being selected depending on the nature and importance of the control. Control tests are designed to evaluate the effectiveness of controls in terms of their design and operating performance. Control tests can include desk based reviews, control walkthroughs, evidence based testing, control observations, independent checking of controls and any other method deemed appropriate.

6.4. Targeted Risk Reviews

The targeted risk review process is used to provide an independent review and analysis of the operation of a selected business function or process. Reviews may be instigated by either the first or second line based on a range of triggers including, but not limited to, KRIs, ILEs, issues and actions and other management information that indicate that there could be an area of potential concern.

Targeted risk reviews are conducted, as appropriate, to identify whether there are any unmitigated risks or inadequacies in control design and provide recommendations to enhance the management of risk. The reviews are generally conducted by the second line of defense and involve various risk management techniques and approaches.

6.5. Key Risk Indicators (KRI)

The Company defines KRIs as metrics that inform users about changes in the frequency or severity of a risk. KRIs are used to monitor all risk categories.

The KRI process is comprised of the following key components:

- KRI development – includes identification of risks and/or controls to monitor using KRIs, selection of a KRI type (lagging or leading), determination of KRI metric and KRI measurement, establishment of thresholds, appointment of a KRI owner and confirmation of sources and availability of data;

- KRI monitoring – includes determination of frequency, monitoring and action and escalation of threshold breaches and validation of thresholds;

- KRI reporting – includes regular reporting at company and unit levels using an established pro-forma; and

- KRI review – includes annual and ongoing review to validate KRIs and assess the ongoing suitability and usefulness of the KRIs monitored.

6.6. Internal Loss Events (ILE)

The collection of ILEs provides meaningful information to better assess the Company's exposure to risk and enhance processes which control the risk. The ILE process applies to the operational risk category. An ILE refers to a materialized risk, caused by the failure of internal processes, people and systems, or from external events.

The ILE process aims to assist the business in identifying and quantifying ILEs, support proactive management of ILEs and create a process for the escalation of ILEs to alert management to areas where action is required.

The ILE process is comprised of a number of key steps as follows:

ILEs with a financial impact of PhP100,000.00 are captured (or as otherwise required by regulatory requirements) and escalated.

ILE Type	ILEs to be recorded
Actual ILEs	ILEs with an estimated gross loss of PhP500,000.00 or greater.
Fortuitous Gains	ILEs with an estimated gross gain of PhP500,000.00 or greater.
Near Misses	ILEs with that could have resulted in a loss or gain of PhP500,000.00 or greater had the ILE not been averted.

ILEs are escalated based on an ILEs estimated impact which ranges to >PhP50,000 or > PhP100,000 and must be escalated to each of the individuals or groups listed below within 5 days of discovery.

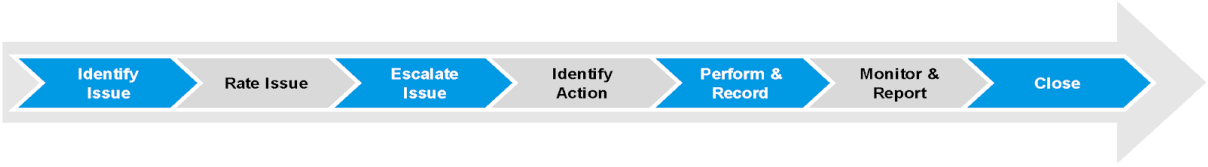
Estimated Loss	Escalation requirements	Timeline
>PhP50,000 to <PhP100,000	▪ Head of Department ▪ Risk and Compliance ▪ President ▪ CEO	Within 5 days of discovery
>PhP100,000	▪ Head of Department ▪ Risk and Compliance ▪ President ▪ CEO ▪ Board of Directors	Within 5 days of discovery

7. ISSUES AND ACTIONS

The Company defines issues and actions as follows:

- an ***issue*** is defined as a problem that needs to be resolved i.e. areas of concerns, weaknesses or improvements to the risk and control environment.
- an ***action*** is a task that needs to be performed as a step towards resolving an issue. Multiple actions can be performed for a single issue.

Many of the risk management processes may result in the identification of issues including risk appetite, RCA, scenario analysis, ILE, and KRIs. The issues and actions process aims to promote the early identification of concerns, weaknesses or improvements to the risk and control environment and ensure proactive escalation and monitoring of issues and actions.



Issues and Actions Process

7.1. Issue Ratings

Issues are rated based on financial and non-financial impact. Issues are assessed based on the potential risk to the Company if the issue is not resolved.

- **Financial -** The financial impact is assessed as the potential risk exposure to the Company if the issue is not resolved. Financial impact is further categorized based on the table below:

Issue Rating	Low	Medium	High	Critical
Financial Impact (PhP)	<25,000	25,000 to <50,000	50,000M to <100,000	>100,000

- **Non-Financial -** Potential non-financial impact is considered based on four factors: reputational impact; regulatory impact; staff health and safety; and business disruption and management effort. A four-level scale applies to each of these factors, as illustrated in the table below.

Impact	Low	Medium	High	Critical
Reputational Impact	Complaints from a relatively small number of stakeholders with no media coverage	Complaints from a small number of stakeholders and/or limited adverse local / state media coverage	A noticeable increase in the volume of stakeholders complaints and/or short- term adverse national or international media coverage	Significant number of stakeholders complaints and/or extended adverse national and or international media coverage
Regulatory Impact	Cautioned or repeatedly cautioned by regulator for minor breaches	Escalation in supervision by regulator resulting in increased reporting requirements	Adverse directive issued by regulator to senior management or board	Sanction from regulator
Staff health and safety	Loss of a staff member from work through injury or illness	Loss of multiple staff members from work through injury or illness	Major injury to staff as a result of a workplace health and safety issue or potential for short-term wide-spread impact on staff	Potential / actual death of staff member(s) or potential for wide-spread impact on staff health or safety
Business disruptions and management effort	Some disruption which can be absorbed through normal management activities	Reprioritization of management activities required and senior management required for decision-making	Reprioritization of management activities required and President & CEO required for decision-making	Redirection of management activities and staff to address the issue. Support (external or otherwise) is required to maintain BAU activities

If the financial and non-financial impacts differ, the greater of the two is used to determine the issue rating. Rating an issue assists prioritization of action and also determines the escalation and oversight required.

Delegated Authorities

Breaches of delegated authority are rated in accordance with the guidance below.

Impact	Low	Medium	High	Critical
Breach	A breach is only marginally outside an individual's authority (i.e. <2% of the applicable limit), is considered to have been unintentional and the quantified risk is negligible	The breach is within the authority of the President & CEO's direct report but outside an individual's authority (subject to the criteria for low impact)	The breach is within the authority of the President & CEO's but outside the authority of the President & CEO's direct report (Product / Business Unit Leads)	The breach is outside the authority of the President & CEO

Risk Appetite and Regulatory Related Matters

Breaches of risk appetite (upper or lower limit) should be rated as either High or Critical depending on the particular circumstances.

All regulatory related matters outlined in section 12.2 should be rated as High or Critical depending on the particular circumstances and escalated in accordance with section 8.2 below.

7.2. Escalation

Issues rated as High or Critical must be escalated to the following:

Rating	Escalation requirements	Timeline
Critical	▪ Head of Internal Audit ▪ Risk and Compliance ▪ Department Head ▪ President & CEO ▪ Board of Directors	Within 5 days of identification
High	▪ Head of Internal Audit ▪ Risk and Compliance ▪ Department Head ▪ President & CEO	Within 5 days of identification

7.3. Monitoring, Reporting, Closure

Issue owners and action owners are required to regularly monitor the progress of their issues and actions and the success of these approaches in addressing the underlying problem or opportunity. Status updates must be provided on all issues and actions and these are used for reporting purposes.

Before an issue or action can be closed, the following conditions must be satisfied:

- the issue must be adequately resolved; and
- the risk must be reduced, transferred, or avoided to the level planned (as applicable).

In certain circumstances, the issue or action can be closed if the risk is consciously accepted by management. All such acceptances must be subject to appropriate governance.

All actions must be completed to the satisfaction of the issue owner before an issue can be closed. The issue owner is responsible for closing the issue. Evidence must be available to substantiate closure of the issue/action.

8. ANNUAL REVIEW

The Company's RMS is reviewed at least annually to ensure that it accurately documents the Company's ERM Framework. This RMS is also reviewed where there are material changes to the operations of the Company to ensure it remains appropriate to address any changes.

The effectiveness of the Company's approach to risk management is reviewed by management on an ongoing basis and reported to the RMC on a regular basis.

Compliance with and effectiveness of the ERM Framework is subject to review by internal and/or external audit at least annually. The results of this review are reported to the Audit Committee and the Risk Management Committee. The appropriateness, effectiveness and adequacy of the Company's ERM Framework are subject to a comprehensive review by an operationally independent, appropriately-trained and competent persons at least every three years.