ENTERPRISE RISK MANAGEMENT

THE PLDT GROUP has long recognized ENTERPRISE RISK MANAGEMENT (ERM) as essential to the achievement of business goals and objectives. The organization acknowledges ERM's role in the promotion of a comprehensive understanding of risks and their effects on overall performance.

GROUP ENTERPRISE RISK MANAGEMENT DEPARTMENT (GRMD)

The commitment of the PLDT Group to the proactive management of existing and emerging risks is reinforced by the Group Enterprise Risk Management Department (GRMD). The GRMD, under the leadership of the Chief Risk Management Officer (CRMO), develops and manages a comprehensive integrated risk management program that is implemented across all levels of the organization.

THE PLDT GROUP RISK MANAGEMENT PHILOSOPHY STATEMENT

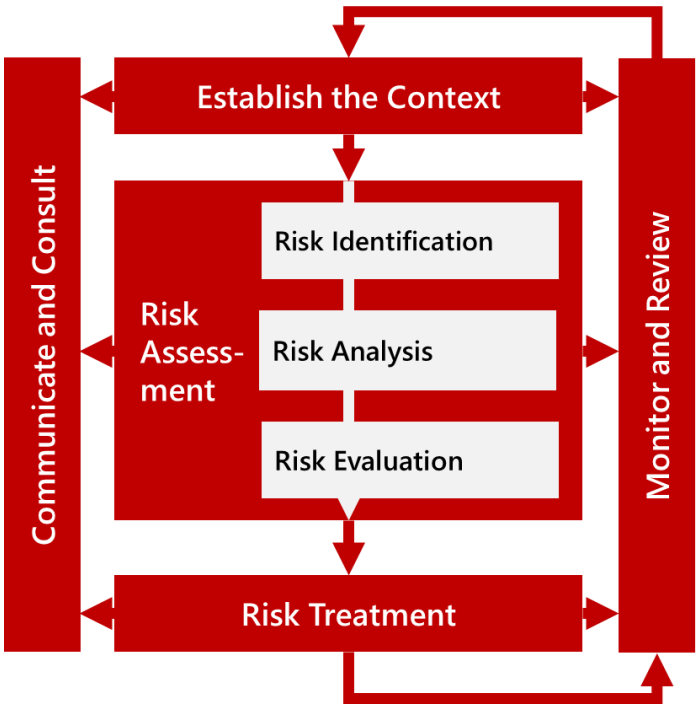
The PLDT Group adopts a risk philosophy that recognizes risks as integral to its business. It commits to enhance shareholder value through proper management of risks, consequently promoting the creation of business opportunities and reduction of threats.

> *The PLDT Group operates in a complex and dynamic business environment which gives rise to a variety of risks that can be both threat and opportunity. Recognizing that these risks are an integral part of its business, the PLDT Group is committed to managing its overall risk exposure in a systematic way and in such a manner that supports its strategic decision-making process. Accordingly, the PLDT Group employs a comprehensive, integrated risk management program, effected across all levels of the organization, with the goal of identifying, analyzing and managing the Group's risks to an acceptable level, so as to enhance opportunities, reduce threats, and thus sustain competitive advantage. The PLDT Group believes that an effective risk management program will contribute to the attainment of objectives by PLDT and its subsidiaries, thus creating value for the business and its stakeholders.*

THE ENTERPRISE RISK MANAGEMENT FRAMEWORK AND PROCESS

The GRMD promulgates and encourages the adoption of a standard risk evaluation process, which properly identifies, analyzes, evaluates, treats and monitors risks that affect the achievement of business objectives. The ERM process currently implemented in the Group is based on the ISO 31000 international standard of risk management.

ISO 31000: Risk Management Process



The implementation of the ERM process ensures that critical risks are well understood and effectively managed across all functions and units within the PLDT Group.

THE PLDT GROUP ERM PROCESS

Establishing the Context

The ERM process forms part of any strategy, business, and budget planning process within the Group. It is initiated and led by the Operational Unit Head, who is assisted by the Risk Coordinator of the unit. Key members of the unit participate by providing necessary input.

The first step of the process requires the articulation of the objectives or priorities of the operational unit. The defined objective must be aligned with overall Group objectives. By clearly setting the business objective, the scope of the ERM process and the external and internal considerations for managing risks will be easily discernible, thus facilitating the rest of the process.

After articulating the objective, the unit must then define its risk appetite and risk tolerance. The operational unit also includes an assessment of potential vulnerabilities in its current fundamental business assets and controls. Metrics must also be put in place to measure and monitor performance of the unit regarding its defined tolerance.

In addition, the state of risk culture in all levels of the Group must be assessed. Risk culture is defined as a set of behaviors and values that shapes risk decisions made by both the Group management and its employees. A strong risk culture consists of a singular awareness and alignment of Group risks at all levels, facilitating the implementation of the overall risk management framework.

Risk Assessment
Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk Identification
The aim of risk identification is to generate a comprehensive list of risks based on events that might create, enhance, prevent, degrade, accelerate or delay the achievement of the business objective. This step requires an intimate knowledge of the organization, the environment in which it operates, as well as an understanding of the organization's strategic and operational objectives. It also includes factors critical to its success, as well as the threats and opportunities related to the achievement of these objectives.

Furthermore, in adherence to the governance structure, the GRMD considers the assessment of fraud risk exposure in its processes to identify specific potential schemes and events that the Group may need to mitigate.

Risk Analysis
Risk analysis involves developing an understanding of the risk by considering potential causes and sources of the risk, its positive and negative consequences, and the likelihood that the risk can occur. In addition, it identifies and evaluates existing controls that respond to the risk, if any, while aiding the Unit Heads in proposing new ones whenever current controls are deemed ineffective.

Risk is analyzed by determining the impact and likelihood of each risk, with consideration of existing controls, using a scale which is outlined in the Risk Impact Guidelines and Risk Likelihood Guidelines defined by the GRMD. Both guidelines require review and calibration at least once a year and are endorsed by the Risk Committee.

For every identified risk, a risk owner must be assigned to ensure responsibility for managing the risk. The analysis is then conducted by determining the impact and likelihood of each risk with consideration of existing controls, using a scale which is defined in the Operational Risk Governance Document.

Risk Evaluation
The purpose of risk evaluation is to assist in making decisions based on the outcome of risk analysis. It determines which risks are prioritized for treatment and escalated to Senior Management and/or the Board of Directors. Risks are classified based on the Group's Risk Assessment Matrix found in the Operational Risk Governance Document.

For critical fraud risks, GRMD will escalate the concern to the Internal Audit Department for appropriate and timely investigation and corrective action.

Risk Response/Risk Treatment
Risk response or treatment involves selecting and implementing one or more treatment strategies to address risks. Suitable risk treatment strategies and action plans must be developed by the operational unit. Options for risk treatment strategies may include:

a. Accepting the risk by informed decision.
b. Avoiding the risk by deciding not to pursue or changing the activity that gives rise to the risk;
c. Treating the risk; and
d. Transferring to or sharing the risk with another party.

Selecting the most appropriate risk treatment strategy involves balancing the costs and efforts of implementation against the benefits derived. Therefore, milestones and performance measure have to be set for the action plans in order to measure their effectiveness.

The risk owner and the treatment plan owner shall be responsible for coordinating and engaging the different teams involved in the implementation of the strategies and action plans. Appropriate resources must be made available to ensure these plans are implemented effectively.

Risk treatment strategies, action plans, accountabilities, and performance measures should be documented.

Monitoring and Review

Depending on the risk score, risks must be reported to the relevant authority. Progress of risk treatment strategies must also be monitored against agreed milestones and performance measures. The risk owner must regularly submit a report to the GRMD indicating the current status of the action plans and progress towards the achievement of the strategy. New or additional risk treatment strategies must be developed by current or different risk owners whenever an agreed strategy is not achieving the intended result.

The monitoring process will also encompass updating the risk assessment considering developments in both internal and external environments. The update must identify additional risks which have emerged since the last review, and also examine all risks in the risk register.

Communication and Consultation

The output from the ERM process must be properly documented. All forms involved in the process will be submitted to and maintained by the GRMD in its risk register. This ERM database will assist in the review of past risk assessments for learning and improving the ERM process and methodologies involved. This, too, will serve as an audit trail for periodic audits by the Internal Audit Department or external auditors to test compliance with agreed upon policies and strategies.

Results of the ERM process must be reported by the GRMD to key stakeholders, particularly to the PLDT Group Top Management Team, the Risk Committee and the PLDT Board of Directors. The report aims to inform these stakeholders of any critical risks that must be managed in the organization so that they can evaluate and provide direction on the appropriate action to address these risks.

Training or workshops will be conducted with the operational units to cascade the ERM process, as the need arises.