

MANUAL	CORP – ERM – 001	
ENTERPRISE RISK MANAGEMENT	Revision No.: 01	Effective Date: March 2026

REVISION HISTORY

Rev. No.	Rev. Date	Description of Change	Author / Originator
00	2019	Initial Issuance	
01	2026	Updated ERM Program	Hu, Bernice Jillian O. Batiancila, Joland Abby R.

ENTERPRISE RISK MANAGEMENT

March 2026

Table of Contents

1. Introduction	6
1.1. About the Manual.....	6
1.2. Scope	6
1.3. Key Objectives of the Manual.....	7
1.4. Definition of Terms.....	7
2. ERM Framework.....	9
2.1. Phase 1: Establishing the Context	10
2.1.1. Leadership Commitment (Tone from the Top).....	10
2.1.2. Group Risk Organizational Structure	10
2.1.3. ERM Process.....	12
2.1.4. Risk Appetite and Tolerances.....	12
2.1.5. Risk Register	13
2.1.6. ERM Maturity Model	13
2.2. Phase 2: Risk Assessment and Treatment	14
2.2.1. Risk Identification.....	14
2.2.2. Risk Analysis	14
2.2.3. Risk Evaluation	16
2.2.4. Risk Mitigation	16
2.2.5. Risk Treatment	17
2.2.6. Control Assessment	17
2.3. Phase 3: Monitoring and Review.....	17
2.4. Phase 4: Communication and Consultation	17
2.4.1. Internal Communication and Reporting	17
2.4.2. External Reporting and Compliance	18

List of Figures

Figure 1: ISO 31000:2018 Risk Management - Guidelines Process	9
Figure 2: 2017 COSO ERM Framework	9
Figure 3: Risk Organizational Structure	11
Figure 4: Risk Heat Map	16

List of Tables

Table 1: ERM Maturity Level	13
Table 2: Risk Likelihood Scale.....	15
Table 3: Risk Impact Scale	15
Table 4: Communication and Reporting Structure	17

Validity and Duration of Use

This Manual shall apply within Megawide Construction Corporation (“Megawide” or the “Company”) and shall remain valid and effective unless revised, amended, or superseded by a subsequent version duly approved by the Board Risk Oversight Committee and the Board of Directors.

A revision number shall be indicated in this Manual for purposes of version identification and document control.

The Chief Risk Officer, or an equivalent position designated by Management, shall be responsible for the maintenance, periodic review, and updating of this Manual.

Copyright Statement

This Manual contains proprietary information of Megawide and is intended to provide guidance on the Company’s Enterprise Risk Management framework. No part of this Manual may be reproduced, disclosed, distributed, or used in any form without the express written permission of the Company. Unauthorized use, copying, or disclosure is strictly prohibited.

Copyright © 2026

Megawide Construction Corporation

Published by:

Megawide Construction Corporation

20 N. Domingo St., Brgy. Valencia

Quezon City, Metro Manila, Philippines 1112

All rights reserved. Except as permitted under applicable copyright laws, no portion of this Manual may be reproduced, transmitted, or distributed by any means without prior written authorization from Megawide.

The Company may publish selected portions of this Manual through official channels (including its website) for governance transparency. Any reproduction, distribution, or use beyond viewing for informational purposes requires prior written consent from the Company.

1. Introduction

This Enterprise Risk Management (“ERM”) Manual (“Manual”) establishes the framework through which Megawide Construction Corporation, together with its related subsidiaries, business units, and other covered entities under the Group’s governance scope (collectively, the “Group”, or the “Megawide Group”), identifies, assesses, manages, and monitors risks that may affect the achievement of its strategic and operational objectives. It provides a structured and consistent approach to managing uncertainty and supports informed decision-making across all levels of the organization. The ERM framework is aligned with the *ISO 31000:2018 – Risk Management Guidelines* and the *2017 COSO ERM Framework* and is integrated into the Group’s governance, strategy, and operational processes.

The ERM framework also supports the Board and Management in evaluating risk-adjusted strategic opportunities, including investments, major projects, and other significant initiatives of the Megawide Group.

1.1. About the Manual

The Megawide Group adopts ERM as an integral part of corporate governance, strategy formulation, decision-making, and performance management. The Group recognizes that effective risk management supports sustainable value creation, protects the interests of stakeholders, and enhances organizational resilience and sustainability.

This Manual serves as the official reference for the Megawide Group’s ERM framework, policies, roles, and processes within its defined scope, and is aligned with the Board Risk Oversight Committee (“BROC”) Charter. It outlines a standardized approach to risk identification, analysis, evaluation, mitigation, treatment, monitoring, and reporting, ensuring consistent application across covered offices and functions.

1.2. Scope

This Manual applies to all subsidiaries, business units, and related parties within the Megawide Group that fall within the scope of the Group’s enterprise risk management framework.

Covered entities are subject to Board-level risk oversight and are required to identify, assess, manage, and report significant risks, exposures, and other material risk matters in accordance with the Group’s ERM framework and governance protocols.

Material risks, emerging threats, and significant exposures shall be appropriately escalated through Management and reported to the BROC, consistent with the Group’s risk governance structure and reporting requirements.

This Manual aims to promote a consistent, coordinated, and enterprise-wide approach to risk management across the Megawide Group while allowing business units to implement risk management practices appropriate to the nature, scale, and complexity of their operations.

1.3. Key Objectives of the Manual

The Manual aims to:

- Establish a structured framework for identifying, assessing, and managing risks that may affect the achievement of the Megawide Group’s strategic and operational objectives;
- Integrate risk considerations into strategy formulation, investments, project development, and day-to-day operations;
- Define clear governance roles, responsibilities, and accountability of the Board and Management in relation to ERM;
- Align risk-taking activities within the Megawide Group’s risk appetite and tolerance levels;
- Promote a strong risk culture and accountability across the Megawide Group;
- Ensure compliance with applicable laws, regulations, and corporate governance standards relating to risk management; and
- Support informed and risk-aware decision-making across all levels of the Megawide Group.

1.4. Definition of Terms

Enterprise Risk Management (ERM)	A process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. ¹
Event	Occurrence or change of a particular set of circumstances. ²
Frequency	Number of events or outcomes per defined unit of time. ²
Impact	The measure of the tangible and intangible effects (consequences) of a risk in the Group. ²
Inherent risk	The level of risk present in an activity, process, or system before any controls, mitigation, or management actions are applied. ²
Likelihood	The chance of something happening. ²
Negative risk	An uncertain event or condition that, if it occurs, has an adverse effect on the achievement of objectives, potentially causing losses, delays, non-compliance, or harm to people, assets, or reputation. ²

¹Committee of Sponsoring Organizations of the Treadway Commission (COSO)

²International Organization for Standardization. ISO 31000:2018 – Risk Management: Guidelines.

Non-inherent risk	Identified risks that are not inherent in nature and typically emerge from specific events, conditions, gaps, or changes in the internal or external environment.
Opportunity	The combination of circumstances expected to be favorable to the objectives. ²
Organization	A person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives. ²
Positive risk	An uncertain event or condition that, if it occurs, has a beneficial effect on the achievement of objectives, such as improving performance, reducing costs, enhancing reputation, or creating new value. ²
Residual risk	Risk remaining after risk mitigation.
Risk	Effect of uncertainty on objectives. ²
Risk appetite	The amount and type of risk that the Group is willing to pursue or retain. ²
Risk criteria	Terms of reference against which the significance of risk is evaluated, based on organizational objectives, and external and internal context, can be derived from standards, laws, policies, and other requirements. ²
Risk mitigation	The process of identifying, assessing, and implementing strategies to minimize or manage the impact of non-inherent risks.
Risk tolerance	The Group's readiness to bear the residual risk in order to achieve its objectives and can be influenced by legal or regulatory requirements. ²
Risk treatment	The process to apply controlled measures to inherent and residual risks.
Threat	Potential source of danger, harm, or other undesirable outcome. ²

¹Committee of Sponsoring Organizations of the Treadway Commission (COSO)

²International Organization for Standardization. ISO 31000:2018 – Risk Management: Guidelines.

2. ERM Framework

The Megawide ERM Framework is aligned with *ISO 31000:2018 Risk Management Guidelines* and the *COSO Enterprise Risk Management Framework (2017)*, and is designed to support compliance with applicable corporate governance requirements, including the *SEC Code of Corporate Governance for Public Companies and Registered Issuers (SEC Memorandum Circular No. 24, Series of 2019)*.

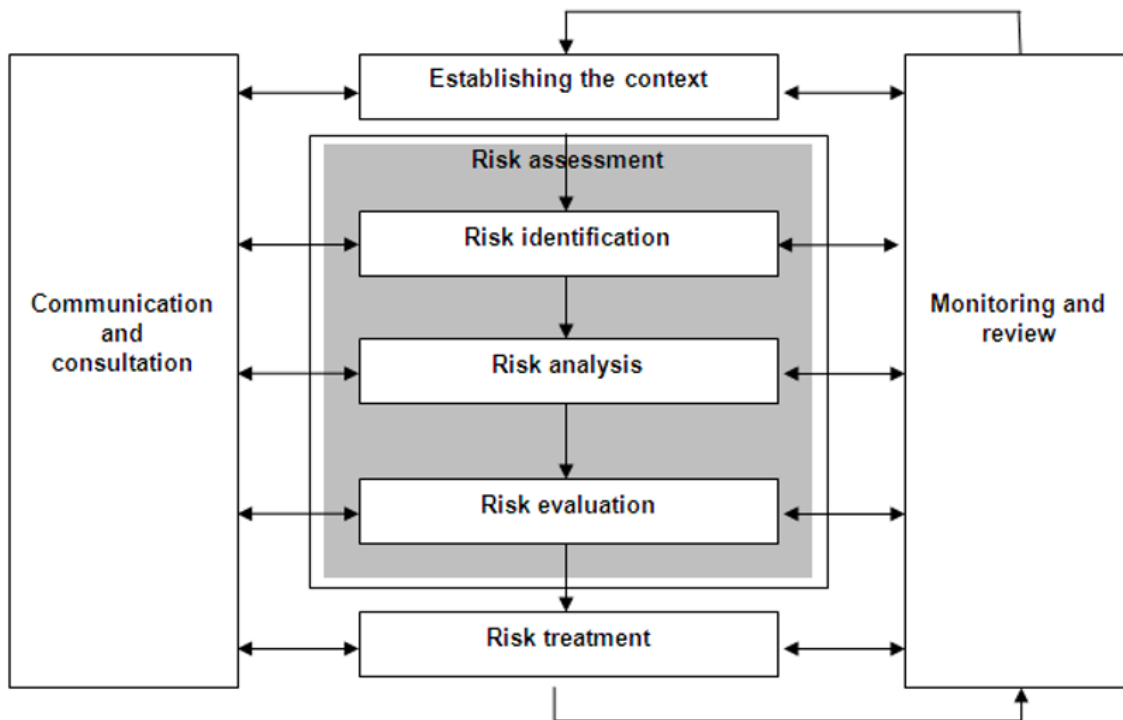


Figure 1: ISO 31000:2018 Risk Management - Guidelines Process



Figure 2: 2017 COSO ERM Framework

The ERM Framework is customized to the Group's external and internal operating environments. Its external environment includes, but is not limited to, the cultural, technological, legal, financial, and regulatory environment, its relationships with stakeholders, as well as industry and international trends. Its internal context includes company culture and values, policies and procedures, guidelines, organizational structure, and such other parameters that are internally driven.

The guidelines and processes set out in this ERM Framework are integrated into the Megawide Group's regular business planning activities. While formal ERM implementation is undertaken on an annual basis, risk management is continuously applied throughout the year through monthly monitoring and reporting, business decision-making, and day-to-day management and operations.

2.1. Phase 1: Establishing the Context

The purpose of establishing the context is to define the environment within which risk management will be applied, enabling effective risk assessment and appropriate risk responses. It involves determining the scope of the ERM process and understanding the external and internal factors that may influence the achievement of the Group's objectives.

The establishment of the ERM system defines the overall structure, governance arrangements, and processes for managing risks across the Group. This includes defining elements such as leadership commitment, risk organizational structure, ERM process, the Group's risk appetite and tolerance levels, risk registers, and the ERM maturity model to ensure a consistent and structured approach to identifying, assessing, managing, and monitoring risks across the organization. Once the ERM system is developed and rolled out, it is subject to periodic review and refinement to support continuous improvement and responsiveness to the Group's evolving risk environment.

2.1.1. Leadership Commitment (Tone from the Top)

Strong leadership commitment is essential to the effectiveness of the Group's ERM Framework. Oversight of the Group's key business risks rests with the BROCC, while Management remains responsible for the identification, assessment, management, and escalation of risks in accordance with the Group's risk governance framework.

Through their oversight role, the Board and the BROCC set the tone for risk-aware governance and promote the integration of risk considerations into strategy, decision-making, and operational management across the organization.

2.1.2. Group Risk Organizational Structure

The Group Risk Organizational Structure defines the governance and accountability framework for ERM across the organization. It establishes clear oversight, leadership, coordination, and operational responsibilities to ensure that risk management is integrated into strategy-setting, decision-making, and day-to-day operations.

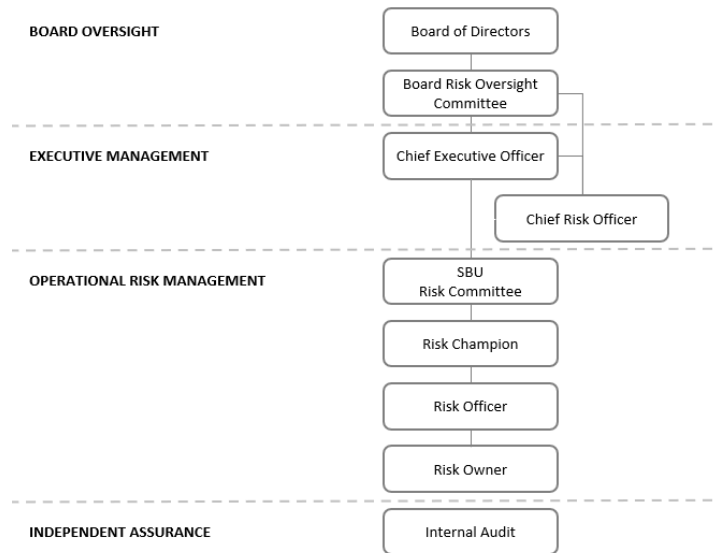


Figure 3: Risk Organizational Structure

At the business unit level, each Strategic Business Unit (“SBU”) maintains its own risk structure by appointing a Risk Champion, Risk Officer, and designated Risk Owners. These roles ensure that risks are consistently identified, assessed, treated, and monitored within each SBU, while maintaining alignment with the Group ERM Framework, risk appetite, and governance requirements.

The BROC provides oversight of the ERM Program, ensures that material risks are appropriately identified, managed, and reported, and reviews consolidated risk exposures against the Board-approved risk appetite.

The Chief Executive Officer (“CEO”) sets the tone for a strong risk-aware culture, ensures ERM is embedded in governance, strategy, and decision-making, aligns actions with risk appetite, empowers the Chief Risk Officer (“CRO”), and ensures accountability and timely escalation of critical risks.

The CRO leads the design, implementation, and continuous improvement of the ERM Framework, coordinates enterprise-wide risk identification, assessment, monitoring, and reporting, guides risk treatment strategies, integrates ERM into strategy and operations, and reports to the CEO, BROC, and the Board.

SBU Risk Committees who are the Management and Executive Committees review and validate risk registers, assess the effectiveness of risk treatments, and monitor significant and emerging risks for escalation.

Risk Champions promote risk awareness and ERM adoption within SBUs, Risk Officers coordinate risk processes and reporting, and Risk Owners are accountable for managing assigned risks, implementing controls, and executing treatment plans.

Internal Audit provides independent assurance on the adequacy and effectiveness of the ERM Program.

2.1.3. ERM Process

The Group's ERM Process provides a structured and integrated approach to identifying, assessing, treating, and monitoring risks that may affect the achievement of organizational objectives. The process is embedded in Management and decision-making across all levels and is applied on a continuous and iterative basis.

The process starts with Risk Identification, followed by Risk Analysis and Risk Evaluation, where risks are assessed against approved risk criteria. Based on the results, appropriate risk treatment or mitigation actions are implemented, and residual risks are reassessed to determine acceptability.

Risks that remain high priority or exceed escalation thresholds are reported to the BROCC for oversight. The process is supported by ongoing recording, reporting, monitoring, and review to ensure risks, controls, and responses remain effective and aligned with the Group's objectives.

2.1.4. Risk Appetite and Tolerances

Megawide Group adopts a disciplined yet enabling risk appetite that supports sustainable growth, innovation, and long-term value creation while safeguarding financial strength, operational reliability, regulatory compliance, and corporate reputation.

The Group recognizes that risk-taking is inherent in pursuing strategic objectives, particularly in construction, infrastructure, and Public-Private Partnership ("PPP") projects. Accordingly, the Group accepts measured and well-governed risks where returns are in proportion with exposures, while maintaining strict limits and thresholds on risks that may compromise safety, legal standing, financial stability, environmental stewardship, or stakeholder trust.

Risk appetite is articulated at three levels:

- Group-level risk appetite, setting overall boundaries for risk-taking;
- Business unit and subsidiary risk appetite, calibrated to the nature of operations;
- Risk category appetite, defining tolerance by type of risk.

Establishing Quantitative Limits

Quantitative limits define the maximum level of risk exposure acceptable to the Group or an SBU and shall:

- Align with the Board-approved risk appetite;
- Be measurable, objective, and regularly monitored; and
- Reflect both normal and stressed operating conditions.

Approval levels:

- Group-wide limits: BROCC
- SBU-specific limits: Risk Committees or the BROCC, as necessary

Establishing Qualitative Limits

Qualitative limits apply to risks that cannot be fully captured numerically but are critical to governance and reputation. These define unacceptable behaviors or outcomes, including but not limited to:

- Deliberate breaches of laws, regulations, or ethical standards,
- Willful compromise of safety or environmental controls, and
- Actions that materially damage stakeholder trust or the Group’s reputation.

Qualitative limits generally operate on a zero or low tolerance basis and require immediate escalation upon identification.

2.1.5. Risk Register

The Risk Register is the primary tool used by the Group to systematically document, assess, and monitor risks that may affect the achievement of strategic, operational, financial, compliance, and project objectives. It consolidates identified risks across the Group, SBUs, and key projects, ensuring a structured and consistent approach to risk management aligned with the principles and process of ISO 31000.

The Risk Register is regularly reviewed and updated as part of ongoing monitoring, periodic risk assessments, and Management reviews. It supports informed decision-making, transparent reporting to Management and the Board, and continuous improvement of the ERM Framework by ensuring that emerging risks, changes in context, and the effectiveness of controls are systematically captured and addressed.

2.1.6. ERM Maturity Model

Maturity Level	Maturity Name	Characteristics and Behaviors
Level 1	Initial	Risk management is informal, siloed, and relies on ad-hoc or corrective actions.
Level 2	Repeatable	Risk management is basic, repetitive processes exist for managing specific risks, though not formally integrated into strategy.
Level 3	Defined	Risk management is systematically implemented across the organization with established, documented guidelines (ISO 31000 standard).
Level 4	Managed	Risk management is integrated with organizational governance, and leadership is committed to risk-based decisions.
Level 5	Optimized	Risk management is fully embedded into the corporate culture, enabling continuous improvement, proactive mitigation, and value creation.

Table 1: ERM Maturity Level

As part of the ERM review process, the Group conducts ERM maturity model assessments, as shown above in Table 1, to evaluate the Group's capability to manage risk, ranging from Initial and Repeatable stages characterized by informal, ad hoc, and reactive practices, through Defined and Managed stages with systematic and governance-integrated risk management, to an Optimized state where risk management is fully embedded, strategic, and value-driven in alignment with ISO 31000. Assessing ERM maturity is an additional input to the annual Board self-evaluation. This process elevates ERM from "management system" to Board accountability. It strengthens alignment with governance expectations defined under the SEC Code of Corporate Governance for Public Companies and Registered Issuers (SEC Memorandum Circular No. 24, Series of 2019).

2.2. Phase 2: Risk Assessment and Treatment

Risk assessment and treatment are essential components of the risk management process under ERM as they provide a structured and systematic basis for managing risks in alignment with the Group's objectives, risk appetite, and risk tolerance, in support of effective governance, informed decision-making, and the consistent management of both potential threats and opportunities.

This phase involves systematic identification, analysis, evaluation, and treatment of risks that may impact the achievement of the Group's objectives. Risks are assessed using established risk criteria to determine their significance and priority. Appropriate risk responses are then identified and implemented in line with the Group's risk appetite and tolerances, with clear ownership assigned to ensure effective risk mitigation and management.

2.2.1. Risk Identification

The risk management process begins with SWOT and PESTEL analyses and through incident reporting, audits, project reviews, and regulatory updates during the strategic planning exercise for regular operating businesses, during which potential risks that may support or hinder the achievement of the Group's objectives are identified and described by Risk Owners. For new businesses or projects, risks are identified at the start. Each risk is then profiled by risk category, subcategory, description, root cause, and potential impact, ensuring a clear definition and consistent classification, and is documented in the Risk Register. Risk responsibility is also assigned by identifying the Risk Owner and the responsible unit, thereby establishing accountability for the Management and ongoing monitoring of each risk.

2.2.2. Risk Analysis

Risk analysis involves assessing risks in terms of likelihood and impact. The analysis may be qualitative, quantitative, or a combination of both, depending on the purpose, data

availability, and complexity of the risk. Results of the risk analysis support risk evaluation, prioritization, and decisions on whether further risk treatment is required.

Risk criteria define the standards used to assess, evaluate, and prioritize risks in a consistent and structured manner across the Group. Risks are assessed based on likelihood (probability of occurrence) and impact (severity of consequences), aligned with the Group’s risk appetite and tolerances. The combined assessment of likelihood and impact determine the overall risk rating and priority level for escalation and treatment.

Likelihood:

Rating	Frequency	Description
4 Very High	More than once per year	The event is expected to occur frequently.
3 High	About once a year	The event is expected during a normal business cycle, likely to occur based on past experiences.
2 Medium	About once every 2–3 years	The event could occur occasionally but is not expected annually. Controls are in place to reduce the likelihood.
1 Low	Once in more than 3 years	The event may occur only in exceptional cases.

Table 2: Risk Likelihood Scale

Impact:

	Financial	Business Interruption	Reputation/ Brand	Health, Safety & Environment	Compliance/ Legal
4 Very High	<ul style="list-style-type: none"> Threatens the viability of SBU/project, may require external financing, restructuring, or divestment. 	<ul style="list-style-type: none"> Interruption of operations for >24 hours¹ Interruption of operations for > 5 working days² 	<ul style="list-style-type: none"> National/international media coverage Loss of investor/client/partner’s confidence 	<ul style="list-style-type: none"> Fatality or permanent disability Severe, irreversible environmental damage 	<ul style="list-style-type: none"> Regulatory suspension, license revocation, litigation Unresolved >1 year
3 High	<ul style="list-style-type: none"> Directly impacts SBU/project annual financial performance, requiring Risk Committee intervention. 	<ul style="list-style-type: none"> Interruption of operations for >12 to 24 hours¹ Interruption of operations for > 4 to 5 working days² 	<ul style="list-style-type: none"> Sustained negative coverage in local press or industry forums Measurable decline in stakeholder trust 	<ul style="list-style-type: none"> Lost time injury or hospitalization to 1 person Moderate environmental damage resolved in 6 months 	<ul style="list-style-type: none"> Formal penalty, sanction, or audit finding, Resolved >6 months to 1 year
2 Medium	<ul style="list-style-type: none"> Requires SBU budget adjustment but does not affect SBU annual target delivery. 	<ul style="list-style-type: none"> Interruption of operations for > 6 to 12 hours¹ Interruption of operations for > 2 to 4 working days² 	<ul style="list-style-type: none"> Negative feedback from limited stakeholders Minimal media mention 	<ul style="list-style-type: none"> Medical treatment case Minor environmental incident resolved in 30 days 	<ul style="list-style-type: none"> Repeated non-compliance, minor notices from regulators Resolved within 6 months
1 Low	<ul style="list-style-type: none"> Absorbed within unit/department budget without affecting targets. 	<ul style="list-style-type: none"> Interruption of operations for <= 6 hours¹ Interruption of operations for 1 to 2 working days² 	<ul style="list-style-type: none"> No external awareness Internal concern only 	<ul style="list-style-type: none"> First aid case No lost time 	<ul style="list-style-type: none"> Minor non-compliance, corrected within 7 days No external notice

Note: (1) Applicable to public-facing SBUs, (2) Applicable to other SBUs other than public-facing

Table 3: Risk Impact Scale

Risk Rating = Impact x Likelihood

LIKELIHOOD	4				
	3				
	2				
	1				
		1	2	3	4
	IMPACT				

Legend:

Code	Description
	1 st Priority
	2 nd Priority
	3 rd Priority
	4 th Priority

Figure 4: Risk Heat Map

The Risk Heat Map translates the combined assessment of impact and likelihood into defined risk priority levels, which determine the appropriate level of escalation, oversight, and Management action.

2.2.3. Risk Evaluation

This process distinguishes the risk type, whether inherent or non-inherent. Inherent risks are risks that arise naturally from the Group’s objectives, activities, and operating environment and exist before the application of any controls. Non-inherent risks are risks that typically emerge from specific events, conditions, gaps, or changes in the internal or external environment. The risk type determines whether the risk proceeds to risk treatment (for inherent risks) or risk mitigation (for non-inherent risks).

Risk evaluation is the step in the risk management process where the results of risk analysis are compared against the Group’s defined risk criteria to determine the significance of each risk and the appropriate course of action.

2.2.4. Risk Mitigation

Risk mitigation applies only to *non-inherent risks*. The resulting priority risks will then be subject to risk mitigation through the introduction of enhancements or strengthening of controls such as policies, procedures, processes, systems, or safeguards.

After mitigation measures are implemented, the risk is reassessed to determine the residual risk. Residual risks that remain high after implementing mitigating controls and measures, together with Inherent risks, are subject to risk treatment and remediation.

2.2.5. Risk Treatment

Risk treatment is the step in the risk management process where only *inherent* and *residual risks* are evaluated to determine how they should be addressed.

During this step, the Risk Committee reviews the inherent or residual risk level against the Group risk appetite and tolerance and determines the most appropriate response.

2.2.6. Control Assessment

Following risk mitigation on non-inherent risk, a control assessment is conducted to evaluate whether existing mitigating controls are adequately designed and effectively operating to reduce the risk to an acceptable level. Control effectiveness is rated using standard categories (e.g., Effective, Needs Improvement, Not Effective) and serves as the basis for determining residual risk, the need for further action, and ongoing monitoring and review.

2.3. Phase 3: Monitoring and Review

This phase ensures that all non-inherent and inherent risks—as well as their corresponding mitigation and treatment plans—are regularly reviewed, updated, and validated for effectiveness. Monitoring and review activities should take place in all stages of the process, enabling Management to evaluate whether implemented mitigation controls and treatment strategies remain relevant, sufficient, and aligned with current business conditions.

The results of monitoring and review should be incorporated throughout the Group’s performance management, measurement, and reporting activities.

The assessment of the Group’s risk maturity level is overseen by the CRO and the BROCC. The CRO provides direction and oversight of the assessment, reviews and validates the results prepared by each SBU Risk Committee, and ensures alignment with the ERM Program.

2.4. Phase 4: Communication and Consultation

This phase ensures the transparent, consistent, and timely dissemination of risk information across all levels. It promotes accountability, reinforces a risk-aware culture, and enables informed decision-making by Management and the Board. Effective communication and reporting also ensure compliance with internal governance standards and external regulatory requirements.

2.4.1. Internal Communication and Reporting

Level	Committee Meeting	Frequency	Agenda
Board	Board Risk Oversight Committee Meeting	Quarterly	CRO-Evaluated Inherent and Residual Risks ERM Program updates; Escalated emerging risks
Executive/ Management	Risk Committee (Executive or Management Committee) Meetings	Once a Month	Priority, Inherent, and Residual Risks per SBU
Departmental/ Functional	Department or Project Meetings	At least twice a month	Risk Register per Department/Project

Table 4: Communication and Reporting Structure

The structure shown in Table 4 defines the hierarchy, reporting flow, and frequency of risk reviews from the Risk Owner up to the Board level. It ensures consistent communication, accountability, and escalation of material risks across the Group.

2.4.2. External Reporting and Compliance

The BROC plays a critical role in supporting the Group's compliance with SEC Corporate governance reporting requirements by providing Board-level oversight of Group risks and the ERM Framework. Through its regular reviews and deliberations, the BROC ensures that material risks, risk management structures, risk appetite, and mitigation strategies are appropriately identified, assessed, and monitored, which form key disclosures in the Annual Corporate Governance Report and SEC Forms 17-A (Annual Report) and 17-Q (Quarterly Report). The BROC's oversight and documented actions demonstrate the Board's active involvement in risk governance, strengthen transparency and accountability, and support accurate, consistent, and credible ERM-related disclosures required by the SEC.

This phase concludes the ERM cycle but also reinforces the continuous improvement of the program. Lessons learned and insights gained from reporting activities are incorporated into subsequent cycles to enhance the Group's overall risk management maturity.

Approved by:

(Sgd.) GIL B. GENIO
Chairman, Independent Director

(Sgd.) CELSO P. VIVAS
Vice Chairman, Independent Director

(Sgd.) EDGAR B. SAAVEDRA
Member

(Sgd.) RAMON H. DIAZ
Member

(Sgd.) ALFREDO E. PASCUAL
Member, Independent Director

On behalf of the Board of Directors:

(Sgd.) EDGAR B. SAAVEDRA
Chairman of the Board

Date Approved: March 18, 2026