Enterprise Risk Management (ERM) Policy

HOWDEN

Document Information & Control

Document Title:	**Enterprise Risk Management (ERM) Policy**
Version:	**1.0**
Effectivity Date:	**30 March 2026**
Document Control No:	**HERMP-03-2026-R00**
Information Classification:	**Level 1 (Limited)**
Review Due:	**March 2027**

Contents

01 Purpose

HOWDEN INSURANCE & REINSURANCE BROKERS (PHIL), INC. ("HIRBPI" or the "Company") has formalized and adopted this Enterprise Risk Management (ERM) Policy to ensure that the Company maintains a sound and effective framework for identifying, assessing, managing, monitoring, and reporting risks that may materially affect the Company's business objectives, financial condition, operational performance, regulatory compliance, and reputation.

The Company recognizes that prudent risk governance is integral to corporate accountability and sustainable operations.

This Policy is adopted pursuant to:

- The Insurance Commission's corporate governance standards.
- Relevant Insurance Commission circulars and advisories.
- The Board's commitment to sound risk governance, prudent risk-taking, and the protection of all stakeholders.
- Howden Group Policy and Standards.

02 Scope

This Policy applies to the Board, Senior Management, officers, and all personnel of the Company. It covers all material risks across the enterprise, including strategic, operational, financial, compliance, information security, reputational, outsourcing, and third-party risks.

Risk management shall be conducted on an enterprise-wide basis and shall not be confined to any single unit, function or activity.

03 ERM Framework

The Company adopts an enterprise risk management framework aligned with internationally recognized standards issued by the International Organization for Standardization, including ISO 31000 and ISO/IEC 27001:2022.

The detailed processes for risk identification, analysis, evaluation, treatment, monitoring, documentation, and continual improvement is set out in the Company's Risk and Opportunity Management Policy.

The Company's Enterprise Risk Management framework is supported by Board-approved operational, compliance, and corporate governance policies governing specific risk domains, including information security, third-party management, regulatory compliance, and internal control. These policies collectively form part of the Company's risk management architecture. This ERM Policy provides overarching governance oversight and Board-level accountabilities.

04 Risk Governance Structure

The Board exercises oversight into the Company's enterprise risk management framework through the Management Team.

The Board shall approve this Policy and any amendments thereto, establish and periodically review the Company's Risk Appetite Statement, ensure that risk management processes are properly designed and implemented, review the Company's enterprise risk profile at least annually, and ensure that material risks

are addressed within approved tolerance levels. Ultimate accountability for risk oversight remains with the Board.

The Management Team through the Risk Manager is responsible for implementing the ERM framework approved by the Board, conducting enterprise risk assessments, maintaining the Enterprise Risk Register, implementing mitigation measures, and escalating material risks to the Board in a timely manner.

Business Unit Heads and designated risk owners are accountable for identifying and managing risks within their respective areas and ensuring that significant exposures are properly reported.

05 Risk Appetite

The Company shall operate within a formal Risk Appetite Statement (Annex “A”) approved by the Board. The Statement defines the level and types of risk the Company is willing to assume in pursuit of its objectives. Risk tolerance thresholds shall be defined therein, and any breach or anticipated breach must be escalated promptly to the Management Team and the Board

The Board shall consider:

- The Company’s business model and size;
- Regulatory and reputational considerations;
- Financial capacity and operational capabilities.

06 Risk Register

The Company shall maintain a consolidated Risk Register, capturing material risks across all functions. The Management Team shall provide periodic reports to the Board summarizing the Company’s top risks, emerging risks, changes in exposure, and the status of mitigation measures

07 Continuous Monitoring

This ERM Policy and the effectiveness of the ERM framework shall be:

- Reviewed annually; and
- Updated as necessary to reflect changes in the Company’s risk profile or regulatory requirements.

Any material amendments shall be subject to Board approval.

08 Training

The Company shall promote a culture of risk-awareness through:

- Appropriate training and awareness programs;
- Clear risk ownership and accountability at all levels.

09 Regulatory Disclosure

Material risk management matters shall be:

- Disclosed in the Annual Corporate Governance Report (ACGR), and
- Reported to the Insurance Commission, as required.

10 Review and Amendments

This Policy shall be reviewed by the Board at least annually and updated as necessary to reflect changes in regulatory requirements, business operations, or risk environment.

11 Effectivity

This Enterprise Risk Management (ERM) Policy together with its Annex “A” - Risk Appetite Statement (RAS) was approved by the Board on 30 March 2026, as evidenced by Board Resolution dated 30 March 2026, and shall take effect immediately thereafter.

12 Annex

Annex A – Risk Appetite Statement (RAS)

Annex A

Risk Appetite Statement (RAS)

Purpose: Outlines the level and type of risk the Company is willing to take in pursuing its business objectives.

Overall Philosophy: The Company maintains a moderate and controlled risk posture, accepting only risks that are understood, assessed, and managed within established tolerance levels, while avoiding exposures that could materially impair financial stability, regulatory compliance, operational continuity, or reputation.

Risk Appetite by Category:

- **Strategic Risk:** Acceptable when aligned with growth objectives and supported by due diligence.
- **Financial Risk:** Low tolerance for exposures that could materially affect liquidity, capital, or profitability.
- **Compliance / Regulatory Risk:** Zero tolerance for non-compliance with laws, regulations, or IC directives.
- **Operational Risk:** Low appetite; requires adequate controls and procedures.
- **Information Security / Data Privacy Risk:** Low appetite; safeguards maintained per ISO 27001 standards.
- **Third-Party / Outsourcing Risk:** Limited exposure; subject to due diligence and monitoring.
- **Reputational Risk:** Very low tolerance for events or actions that could damage credibility or stakeholder confidence.
- **Risk Tolerance and Escalation:** Material breaches or anticipated breaches of risk thresholds must be escalated promptly to Senior Management and the Board.
- **Review:** This RAS shall be reviewed at least annually to ensure alignment with strategy, regulatory requirements, and business conditions.

Version Control

Version:	Nature of Changes:	Prepared by:	Approved by:	Date:
1.0	First Issuance	Atty. Emmanuel G. Villanueva	Board of Directors	30 March 2026