ZANTAT HOLDINGS BERHAD

(Registration No. 202101040483 (1440783-X))

ENTERPRISE RISK MANAGEMENT (ERM) POLICY

Version 1	Adopted on 25 November 2025

1.0 POLICY STATEMENT

1.1 Zantat Holdings Berhad ("**ZHB**" or the "**the Company**") and its subsidiaries and associate companies (collectively known as "**Zantat Group**" or the "**the Group**") is committed to establishing and maintaining a robust Enterprise Risk Management ("**ERM**") approach and supporting ERM Framework that enable the achievement of its strategic objectives and strengthen long-term organisational resilience.

1.2 The Group recognises that risk is inherent in all business activities. Effective risk management enables informed decision-making and strengthens governance, compliance and stakeholder confidence.

1.3 The Board of Directors has overall responsibility for ensuring that a sound Enterprise Risk Management policy ("**Policy**") and Framework are established, maintained, and periodically reviewed. Management is accountable for implementing the Framework and embedding risk management practices throughout the organisation in accordance with this Policy.

2 OBJECTIVES

2.1 This Policy sets out to achieve the following objectives:

a. to integrate risk management into strategic and operational processes by embedding risk identification, assessment, response, and monitoring across all business units and subsidiaries;

b. to define clear governance and accountability by establishing roles, responsibilities, and ownership for risk management at every organisational level;

c. to enable the Group to take informed decisions that balance risk and opportunity in pursuit of sustainable growth, innovation, and competitive advantage under prudent controls;

d. to ensure continual relevance and effectiveness by periodically reviewing and enhancing the ERM Framework in response to changes in the business environment, regulatory requirements, and stakeholder expectations.

3 SCOPE OF THE POLICY

3.1 This Policy applies to the Group and all its business units, and functional departments. It also extends to associate companies or joint ventures where the Company has management control or significant influence.

3.2 The Policy applies to all directors, employees, and any third parties (including consultants and contractors) engaged to perform work for or on behalf of the Group.

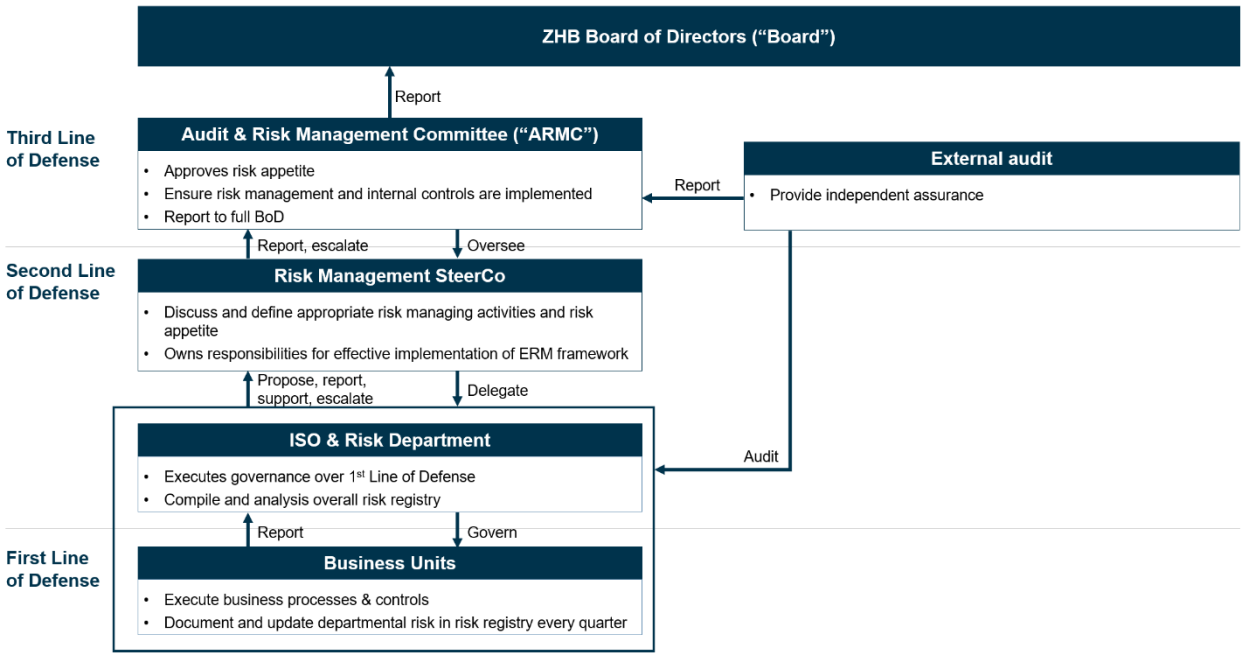
3.3 It covers all categories of risk that may affect the achievement of the Group's objectives, including but not limited to:

Categories	Definitions
Strategic	Risk that adversely affects the stability and/or integrity of the Group as well as its ability to achieve strategic goals and objectives.
Financial	Risks associated with adverse impacts on the Group's financial performance and stability including incurring additional/increased liabilities.
Operations	Risks associated with inadequacy or failure of internal processes, people, and systems, or from external events, causing losses, delays or disruptions to production process or operations of the business and/or key assets.
Health & Safety	Risks associated with the potential harm or danger to the physical well-being and safety of individuals due to hazards, conditions, or activities, both on-site and in any company-related activities.
People & Talent	Risks related to workforce capability, succession planning, and employee well-being.
Reputation	Risks associated with adverse impact to the Group's image, public perception and creditability among its stakeholders, including clients, investors, regulatory bodies, and the public.
Regulatory & Compliance	Risks arising from non-adherence to laws, relevant regulatory requirements, contractual obligations, and industry standards. (e.g. environmental regulations, labour laws, specific industry compliance requirements, etc.)
Environmental	Risks related to environmental performance, pollution, and resource management.
Climate-related	Climate-related risks including physical risks (acute and chronic) arising from climate impacts, and transition risks arising from regulatory, technological, and market changes during the shift to a low-carbon economy.

4 ERM GOVERNANCE STRUCTURE

The Group adopts the Three Lines of Defence model as the foundation of its risk management governance structure, drawing reference from the principles and guidelines of ISO 31000.

4.1 The ERM governance structure defines the roles and responsibilities of the stakeholders in governing, managing, monitoring, and communicating the risks. The Board is responsible for the supervision and monitoring the principal and strategic risks through Audit & Risk Management Committee ("ARMC") while the Risk Management SteerCo is responsible for the overall implementation of risk management across the Group. The governance structure for the Group is shown in the diagram below:

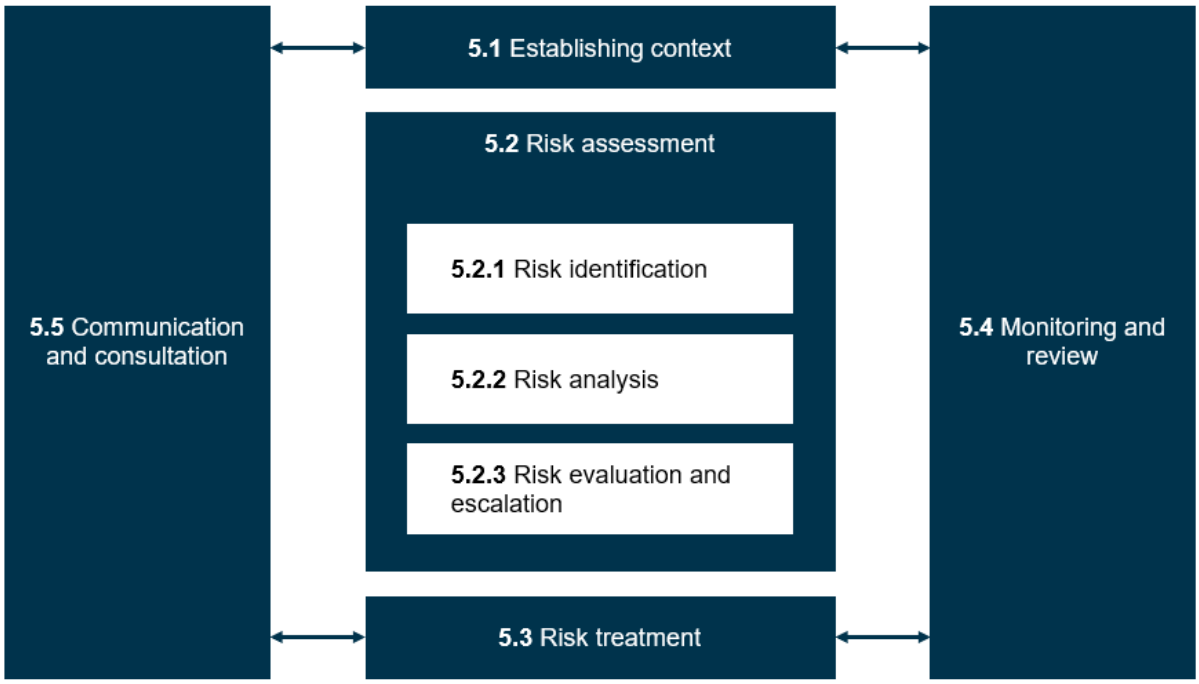


4.2 To ensure adequate governance over the Group's risk management system, the detailed ERM roles and responsibilities are defined as follows

Roles	Key Responsibilities for ERM
Board of Directors ("Board")	• Approves the ERM Policy and risk appetite statement. • Oversees the effectiveness of the ERM approach and/or framework. • Reviews key risks that may affect strategic objectives. • Ensures alignment of ERM with the Group's governance and strategy.
Audit & Risk Management Committee ("ARMC")	• Reviews and monitors the adequacy of the ERM framework. • Advises the Board on risk matters and internal control effectiveness. • Reviews risk reports and significant risk exposures. • Ensures corrective actions are implemented for key risks.
External Audit	• Review the adequacy and effectiveness of the ERM and Group's internal control system. • Provide an independent view and recommends to the Board on the steps to improve the system of internal control derived from the findings of internal and external auditors.
Risk Management Steering Committee ("Risk Management SteerCo")	• Implements the ERM Policy and framework across the Group. • Identifies, assesses, and manages significant risks. • Reviews Group Risk Register and mitigation plans. • Reports risk exposures and updates to the ARMC.
ISO & Risk Department	• Coordinates the Group's risk management processes and documentation. • Consolidates risk reports and maintains the centralised Group Risk Register. • Provides training, awareness, and advisory support on ERM practices. • Monitors implementation of risk mitigation measures.
Business Units / Risk Owners	• Identify and manage risks within their functional areas. • Maintain department-level risk registers and monitor control effectiveness. • Escalate significant or emerging risks to Management. • Comply with the ERM Policy and related procedures.

5 ERM FRAMEWORK AND PROCESS

The Group's ERM Framework references the ISO 31000:2018 Risk Management Guidelines to facilitate the effective identification, assessment, evaluation, treatment, monitoring, and reporting of enterprise and operational risks. The overview and interrelations of the ERM Framework components are illustrated below.



5.1 Establishing context

This stage involves assessing and understanding the business processes and the internal and external factors to be considered when managing risk and sets the scope and criteria for the remaining process:

- **Internal factors:**
  This refers to factors which influence the way of businesses and resources are managed in achieving the Group's mission, vision, values, and strategic objectives. The scope of internal factor includes (but not limited to) internal stakeholders, governance, process, and system.

- **External factors**
  This refers to the macro-environmental factors which influence the business strategy and direction forward of the Group. The scope of external factor includes (but not limited to) relevant social, economic, technological, environmental, regulatory, legal and, geopolitical factors.

5.2 Risk assessment

Risk assessment is a critical component of the Group's ERM Framework. It enables the systematic identification, assessment, management, and mitigation of risks across all levels of the organisation. The Group applies a bottom-up approach, empowering business units to actively identify and assess risks arising from their day-to-day operations.

Each business unit / head of department is responsible for maintaining a departmental risk register, which is updated twice a year or whenever significant changes occur. These registers are consolidated into a centralised Group risk registry maintained by the ISO & Risk Department, which analyses and validates the information before escalation to Management and relevant committees.

5.2.1 Risk identification

Risks are identified through structured methods such as process reviews, incident analyses, and audits. It is important to note that a risk represents a potential future event that may have a positive or negative effect on objectives.

For each risk, the following elements should be clearly defined should be clearly defined to ensure consistency and understanding across the organisation:

- **Source or cause**: what could trigger the event described in specific and factual terms (i.e., customer A with liquidity constraint);
- **Event**: what could happen with brief description of the risk in simple, understandable language across all relevant stakeholders; and
- **Potential consequences**: a brief note on the likely outcome or effect should the event occur (the detailed impact scoring will be performed during risk analysis).

5.2.2 Risk analysis

The likelihood of occurrence and the impact or consequence are assessed to determine the risk rating/score before any mitigation is applied.

- **Likelihood:**

Likelihood represents the probability of a risk event occurring within a defined assessment period, which in the Group's case is twice a year (i.e., every 2 quarters), consistent with the update frequency of the Group Risk Register. For chronic or long-term physical risks (e.g., climate-related), the timeframe for potential trigger is considered in years rather than quarters.

The likelihood assessment considers historical data, management experience, control effectiveness, and the operating environment to estimate how often a risk could materialise. The likelihood scoring is guided by the following scale:

		Chance of happening				
Risk category	**Metrics**	**Low [1]**	**Mid-low [2]**	**Moderate [3]**	**Mid-high [4]**	**High [5]**
Financial **Strategic** **Customer & key account** **Reputation** **Regulatory & compliance** **Health & safety** **People & talent** **Operation** **Environmental** **Acute physical risk** **Transitional risk**	**Chance of happening in the next 2Qs**	≤ 10% once	≤ 25% once	≤ 50% once	> 50% once	> 50% multiple times
Chronic physical risk	**Potential timeframe until event triggers**	> 10 years	5 ~ 10 years	3 ~ 5 years	1 ~ 3 year	Recurring within 1~ 3 year

- **Impact:**
  Impact represents the extent or severity of consequences that would result if a risk event were to occur. Impact assessment is performed per incident within the next two quarters, in line with the Group's twice a year risk-assessment cycle. For long-term or climate-related exposures (such as chronic physical or transition risks), impact is measured based on the projected magnitude of loss or disruption once the event triggers, rather than immediate short-term effects.

  Each risk is evaluated using the Group's category-specific metrics to ensure consistent and objective assessment across all business units:

Directly escalate to ARMC if impact score is 5

Level of risk

Risk category	Metrics (per incident in next 2Qs)	Low [1]	Mid-low [2]	Moderate [3]	Mid-high [4]	High [5]
Financial	Additional cash require	≤ RM200k	≤ RM500k	≤ RM1mil	≤ RM2mil	> RM2mil
	Profit impact	≤ RM50k	≤ RM250k	≤ RM500k	≤ RM1mil	> RM1mil
Strategic	Delay to critical milestones	≤ 2 weeks slip	2 – 8 weeks slip	2 – 3 months slip	3 – 6 months slip	>6 months slip
	Scope change	No scope change	Minor scope change	Moderate scope change	Major scope cut / postpone	Cancellation of initiative
Customer & key account	Potential revenue impact	No revenue at risk	≤ RM250k	≤ RM500k	≤ RM1mil	> RM1mil
	Customer account at risk[1]	Single isolated complaint only	Minor account at risk	Formal complaint; priority account at risk	Formal complaint; priority account at risk	Formal complaint and termination; priority account at risk
Reputation	Bad PR coverage	Internal issue, no external visibility	Local community mention	National coverage	Sustained national coverage	National / international focus
Regulatory & compliance	Action by authority	Informal enquiry	Warning / advisory letter; corrective action required	Warning / advisory letter; corrective action required	Special audit	License suspension / revocation
	Compound / fines	No fine	No fine	≤ RM10k	≤ RM100k	> RM100k
Health & safety	Medical attention needed	First-aid case only	Medical treatment required (clinic visit only)	Medical treatment required (hospitalisation)	Permanent disability	Fatality(ies) case
	Lost-Time Injury (LTI)	No LTI	No LTI	≥ 1 LTI	Multiple LTIs	Multiple LTIs
People & talent	Critical role coverage	Successor is ready; 0 - 2 weeks capability gap	Successor identified; ≤ months capability gap	No identified successor; however temporary cover available	No identified successor	No identified successor and role is business-critical
Operation	Production downtime	≤ 2 hour	≤ 8 hour / half day	≤ 1 day	≤ 2-6 day	> 1 week
Environmental	Extent of impact	Within permit (not considered as offense)	Contained onsite	Limited offsite impact	Significant offsite impact, official regulators involved	Major long-term harm, official regulators involved
	Clean up effort required	No cleanup required	Cleanup costs ≤ RM1k	Cleanup costs ≤ RM10k	Cleanup costs ≤ RM100k	Cleanup costs > RM100k
Acute physical risk	Production downtime	≤ 2 hour	≤ 8 hour / half day	≤ 1 day	≤ 2-6 day	> 1 week
Transition risk	P&L impact	≤ RM50k	≤ RM250k	≤ RM500k	≤ RM1mil	> RM1mil
Chronic physical risk	Effective total production capacity loss (once event triggers)	≤ 2%	≤ 5%	≤ 10%	≤ 20%	> 20%

- **Risk scoring:**

  The combination of Likelihood and Impact ratings produces the overall risk score, ranging from 1 to 25. This score is used to determine the risk level, treatment priority, and escalation pathway, as defined in the Group's escalation matrix.

5.2.3 Risk evaluation and escalation

Risk evaluation involves interpreting the final risk scores to determine their escalation pathway. Each risk is compared against the Group's risk appetite and escalation thresholds, ensuring that material exposures are addressed at the appropriate governance level.

The detailed escalation thresholds by risk category are shown in the table below:

RD Escalate to Risk Department SC Escalate to Risk SteerCo AR Escalate to ARMC Directly escalate to ARMC if impact score is 5

		Escalation threshold													
Risk category	**Coverage**	**1**	**2**	**3**	**4**	**5**	**6**	**8**	**9**	**10**	**12**	**15**	**16**	**20**	**25**
Financial	Effects on P&L and cash flow					RD		SC			AR				
Strategic	Risks that derail approved strategy, major capex initiatives, market positioning										RD SC			AR	
Customer & key account	SLA / service failures, major complaints, credit exposures, loss of key/anchor accounts									RD	SC			AR	
Reputation	Adverse media / analyst / NGO attention affecting stakeholder trust or valuation									RD	SC			AR	
Regulatory & compliance	Breach of law, license, Bursa / MCCG rules, permits, binding internal policies						RD		SC				AR		
Health & safety	Employee safety, health and wellbeing						RD		SC				AR		
People & talent	Critical talent / succession for key roles										RD SC				AR
Operation	Plant / equipment downtime, process failures, supply/logistics interruptions											RD	SC		AR
Environmental	Spills, emissions, permit exceedances, biodiversity / land / water impacts and clean-up										RD SC			AR	
Chronic physical risk	Gradual, longer-running climate stresses that erode performance over weeks / months									RD		SC			AR
Acute physical risk	Short, severe weather events that interrupt operations or damage assets										RD SC			AR	
Transition risk	Policy, legal, tech, market or stakeholder shifts tied to decarbonization / ESG that hit economics or viability									RD		SC			AR

5.3 Risk treatment

Following evaluation and escalation, the Group selects and implements suitable risk-treatment options to modify identified risks in accordance with their assigned priority and escalation pathway.

Treatment options include:

- **Avoiding** the risk by discontinuing or altering the activity that gives rise to it;
- **Reducing** the likelihood or impact through additional preventive or corrective controls;
- **Transferring** the risk through insurance, outsourcing, or contractual arrangements; or
- **Accepting** the risk only when it falls within the Group's approved risk appetite and is formally endorsed by the appropriate escalation authority (e.g., Risk Steering Committee or ARMC depending on the risk level)

Each treatment plan shall identify the responsible risk owner, required resources, target completion date, and key performance indicators to measure effectiveness. Residual risks are reassessed to confirm that exposures remain within approved thresholds.

Progress of risk-treatment plans is monitored by the ISO & Risk Department and reported to Management and the relevant committees.

5.4 Monitoring and review

Risks across the Group shall be reviewed, monitored, and re-evaluated by the respective risk owners on a twice a year basis, with facilitation from the ISO & Risk Department for respective business units.

Risk reviews shall be conducted through structured discussions with business unit risk owners, and any changes arising from these reviews must be updated promptly in the centralised Group Risk Register, which serves as the main repository for risk information.

To ensure effective monitoring, Key Risk Indicators (KRIs) should be established and tracked for all Critical-rated risks *(refer Section 6.0 for the detailed KRI process)*, defined as risks that have been escalated to the Risk Management SteerCo and/or the ARMC, due to their material impact on the Group.

Lessons learnt from incidents, audits, and reviews shall be incorporated into continuous improvement initiatives to strengthen the Group's risk management maturity and resilience.

5.5 Communication and consultation

Regular risk communication/reporting is an integral part of governance which instituted at various levels of the organisation to support oversight bodies in fulfilling the responsibilities. The frequency of reporting to the respective oversight bodies are practiced as follows:

Reporting Party	Reporting to	Reporting Frequency	Report to be submitted
Risk Management SteerCo	• Board • ARMC	Twice a year	• Risk action plans and Key Risk Indicators updates for Top 10 risks • Updated risk appetite statement
Risk Management SteerCo	• Board • ARMC	Ad-hoc	• Special risk report on need basis (i.e., when Key Risk Indicators have been breached)
ISO & Risk Department	• Risk Management SteerCo	Twice a year	• Updated centralised Group Risk Register • Risk action plans and Key Risk Indicators updates for Top 10 risks • Status progress update on the key risk action plans
ISO & Risk Department	• Risk Management SteerCo	Ad-hoc	• Special risk report on need basis (i.e., when Key Risk Indicators have been breached)
Business Units / Risk Owners	• ISO & Risk Department	Twice a year	• Updated risk register and risk profiles of each business unit / department • Detailed risk action plans and status updates
External Audit	• ARMC	Twice a year	• Independent report on the effectiveness of internal controls and risk management implementation

Effective communication and consultation are continuous activities that occur throughout the risk-management process. They ensure that relevant stakeholders understand the basis for risk decisions and that accurate, timely information is shared across all levels of the organisation.

6 KEY RISK INDICATOR ("KRI")

KRI identification process involves identifying existing measurable metrics linked to the risk. The KRI could be either leading indicators or lagging indicators. A well-balanced combination of leading and lagging indicators is important to ensure effective risk monitoring as the leading indicator is predictive in nature that provides early signals of potential risk escalation while lagging indicators offer insights into the historical data which will help in identifying the risk trends.

The KRIs proposed by risk owners shall be validated by the Risk Management SteerCo to ensure relevance, reliability, and consistency across the Group.

Once appropriate indicators have been identified, risk owners shall establish trigger thresholds for each KRI based on the Red, Amber, and Green limits, as defined below:

KRI trigger	Definition
Green	• Green represents a safe or acceptable zone. • When a KRI is within the green limit, it indicates that the associated risk is within acceptable limits. • No immediate action is required.
Amber	• Amber is a cautionary or moderate-risk zone. • When a KRI enters the amber limit, it suggests that the associated risk is approaching a level of concern. • This should prompt closer monitoring and consideration of proactive measures to prevent further deterioration.
Red	• Red indicates a critical or high-risk zone. • When a KRI exceeds the red threshold, it signifies that the associated risk has surpassed the Group's acceptable tolerance and requires immediate management attention. • Action plans and mitigation measures shall be activated. • The relevant governance bodies, according to the defined escalation threshold, shall be informed promptly.

Threshold settings shall be aligned with the Group's Risk Appetite Statement, providing a clear basis for determining the acceptability of risk exposures. Response actions must be defined for both Amber and Red trigger levels to ensure that timely and adequate measures are in place to prevent further escalation of risk exposure.

The status of established KRI shall be reviewed and monitored by the risk owner based on agreed frequency or the frequency of the data available for the indicators.

7 CONTINUOUS IMPROVEMENT AND CAPACITY BUILDING

The Group is committed to the continuous improvement of its ERM Framework and practices. Regular evaluation and enhancement of the ERM processes ensure that they remain effective, relevant, and aligned with the Group's strategic objectives, operating environment, and stakeholder expectations.

Improvement initiatives may include, but are not limited to:

- Periodic review of the ERM Framework and related procedures to reflect emerging risks, regulatory updates, and industry best practices;
- Incorporating feedback and lessons learnt from incidents, audits, and assurance reviews;
- Benchmarking against peer organisations and relevant standards such as ISO 31000; and,
- Conducting training and awareness programmes to strengthen risk culture and capability across all levels of the organisation.

The ISO & Risk Department shall coordinate continuous improvement initiatives and recommend enhancements to the Risk Management SteerCo for endorsement and implementation.

8 PERIODIC REVIEWS

This ERM Policy will be reviewed at least once every 2 years or as and when required to ensure effectiveness and compliance with the governing legislation and regulatory requirement.

9 BOARD APPROVAL

This ERM Policy was approved by the Board of Directors on 25 November 2025.