Enterprise Risk Management (ERM) Framework

GROUP POLICY

Document Summary

Published Date	May 2026
Last Reviewed Date	August 2026
Next Review Date	August 2027
Version	2.0
Author(s)	Strategy & Investment
Approver	Risk Committee

Version Control

Date	Author	Version	Description of changes
2026	Strategy & Investment	1.0	Creation of Enterprise Risk Management Framework
2026	Strategy & Investment	2.0	1. Updated the Combined Assurance paragraph 2. Added Social Risk in sample risk categories

Contents

1. PURPOSE

The purpose of this framework establishes a structured and consistent approach to identifying, assessing, responding to, and monitoring the risks that may affect the achievement of ER Group's objectives. The framework safeguards value, supports informed decision-making, and strengthens organisational resilience by embedding risk awareness into governance, planning , and day-to-day operations. It defines roles, responsibilities, and processes required to manage risks proactively, and ensures that material exposures are escalated, mitigated, and reported to the Risk Committee in a timely and effective manner.

2. OBJECTIVE

This policy aims to:

- Enhance proactive risk management,
- Facilitate risk-based decision making,
- Improve governance and accountability,
- Enhance credibility with wide range of stakeholders,
- Protect and enhance stakeholder value.
- The policy supports innovation while ensuring AI systems are deployed in a controlled, accountable, and trustworthy manner.

3. SCOPE

This policy applies to:

- ER group entities, subsidiaries and business units
- All employees,

I. Enterprise Risk Management Framework

Risk, as defined by COSO, *"is the possibility that events will occur and affect the achievement of strategy and business objectives"*. Enterprise Risk Management (ERM) is defined as *"the culture, capabilities, and practices, integrated with strategy-setting and performance, that organisations rely on to manage risk in creating, preserving, and realising value".*

As a highly diversified conglomerate, ER Group faces a broad spectrum of risks spanning strategic, operational, market, financial, health and safety, and environmental domains. The Group is dedicated to cultivating a culture where risks are identified early, managed effectively, and monitored and reported on an ongoing basis. The Group-wide Enterprise Risk Management (ERM) framework serves as the cornerstone for sustaining this approach to risk governance.

Through this document, ER Group:

- Mandates its commitment to ERM,
- Seeks to embed ERM into the Group's culture by instilling ERM in its process, people and technology.

Through the establishment of an ERM framework, the Group aims to realise the following benefits:

- Enhance proactive risk management,
- Facilitate risk based decision making,
- Improve governance and accountability,
- Enhance credibility with wide range of stakeholders,
- Protect and enhance stakeholder value.

1.1 Long term strategy

"ER Group's ambition is to shape tomorrow by leading responsibly, uniting strengths, and expanding horizons."

ER Group recognises that effective risk management is a cornerstone of long-term resilience and value creation. By proactively identifying, assessing, and mitigating risks, the Group enhances its capacity to withstand disruptions, adapt to change, and capture new opportunities. The ERM framework plays a critical role in safeguarding operational continuity, financial health, and stakeholder interests, while supporting strategic decision-making at every level of the organisation.

Business context analysis

In line with COSO 2017, ER Group conducts an annual business context analysis prior to reviewing risk appetite. This encompasses:

External environment — macro-economic conditions, regulatory developments (including AI and data protection legislation), industry and competitive landscape, technological disruption, climate and ESG trends, and geopolitical developments affecting the Group's operating regions.

Internal context — Group strategy and objectives, organisational structure, financial position, operational capabilities, talent, technology landscape including AI systems in use, and outputs of prior risk assessments. Findings are tabled to the Risk Committee annually and inform updates to risk appetite and the Group risk register.

1.2 Overview of ER Group's clusters

Clusters	AGRIBUSINESS	REAL ESTATE	HOSPITALITY & TRAVEL	LOGISTICS	FINANCE	COMMERCE & MANUFACTURING	TECHNOLOGY & ENERGY
SECTORS	Sugar Cane Food Crops Livestock Agri Services	Homes Workplaces Malls Territories	Hotels Leisure Aviation & Travel Services	Cross-Border Logistics Landside Logistics Packing & Shipping	Credit Fiduciary Leasing	Automotive Trade & Manufacturing	Technology Energy Innovation

1.3 Applicability of ERM

This ERM framework is applicable to ER Group and its subsidiaries. The applicability of ERM is detailed as under:

- Group – Managing risks that affect objectives of the Group. To this extent, ERM at Group level will involve:
  - Identifying, assessing, measuring, consolidating and managing risks emanating from various clusters as well as Corporate Service functions which impact Group objectives.
  - Identifying, assessing, measuring, consolidating and managing risks which exclusively affect the Group objectives.
- Clusters - Identifying, assessing, measuring, consolidating and managing risks that affect the objectives of each material subsidiary in the above identified clusters.

1.4 Risk appetite statements

Risk appetite statements define the nature and extent of risks that an organisation or Group is willing to accept in pursuit of its objectives and business goals. Risk appetite is communicated by management, endorsed by the board, and disseminated throughout the entity. Risk appetite places various risks along a continuum ranging from lower to higher. In addition, ER Group recognises Artificial Intelligence (AI) as an emerging and distinct risk domain. The Group has a high appetite for leveraging AI to drive operational efficiency, customer insight and innovation, while maintaining AI-related risks at a tolerable risk level. AI risk appetite is reviewed annually by the Risk Committee as the regulatory and technology landscape evolves.

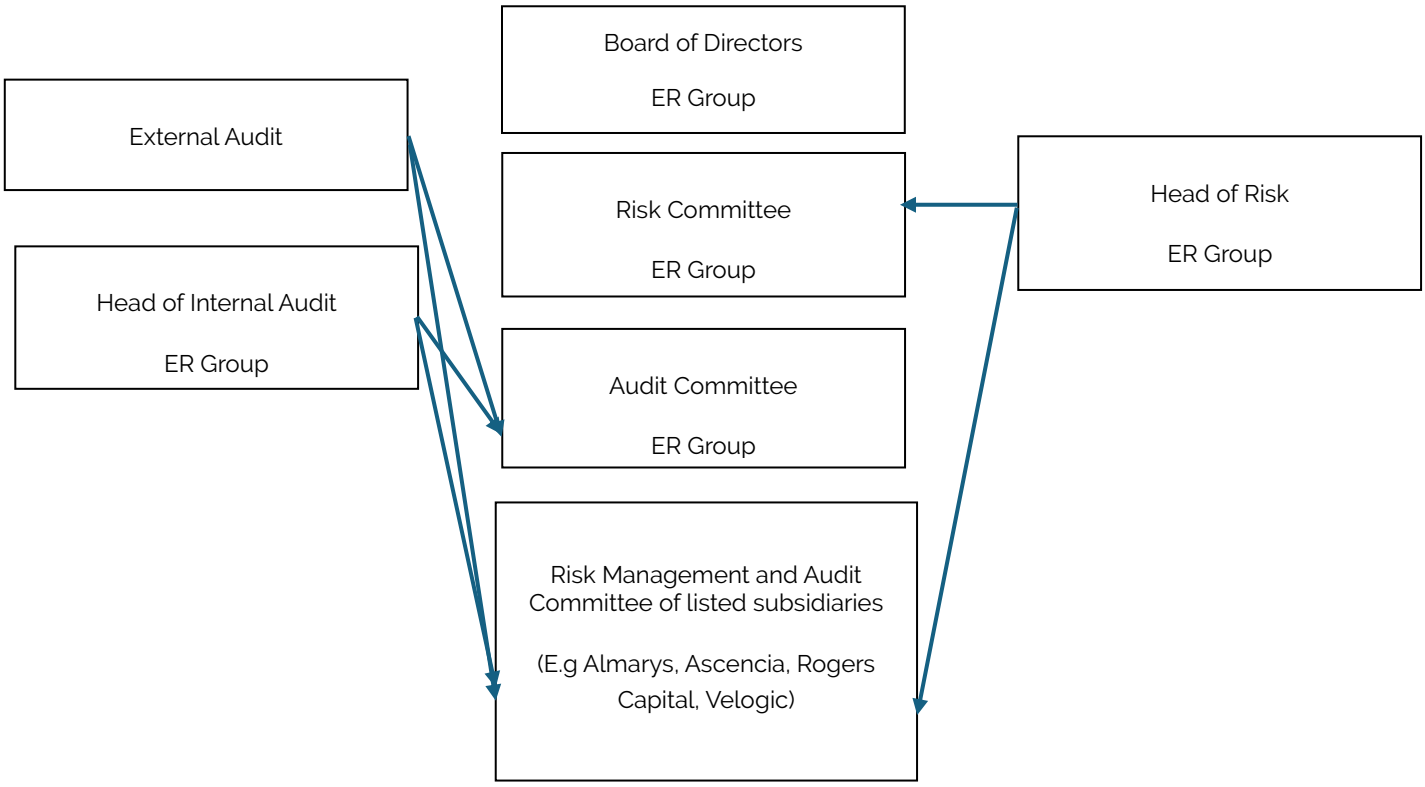
Strategic pillar	Risk appetite statement
Customer Centricity	▪ We have a very high appetite for initiatives that materially improve customer experience, satisfaction and loyalty, including the use of data analytics and emerging technologies to deliver personalised and differentiated experiences. ▪ We have a high appetite for innovation in products, services and customer journeys, provided consistency of experience across subsidiaries is maintained. ▪ We have a very low appetite for risks that could compromise customer trust, including data privacy breaches, cybersecurity incidents, misleading communications or regulatory non-compliance. ▪ We have a low appetite for practices that create inconsistent customer experiences across businesses or dilute the Group brand.
Sustainability & Stewardship	▪ We have a very high appetite for transforming business models, operations and value chains to embed sustainable, ethical and inclusive practices, including energy transition, circular economy and biodiversity initiatives. ▪ We have a high appetite for active engagement in vulnerable communities and national development initiatives, aligned with the Group's stewardship role. ▪ We have a very low appetite for risks that could result in environmental harm, breaches of sustainability regulations, ethical failures, or material stakeholder dissatisfaction. ▪ We accept moderate risks when adopting new sustainable practices or technologies, provided impacts are well assessed and aligned with long-term value creation and trust.
Operational Excellence	▪ We have a very high appetite for innovation, process optimisation and the adoption of emerging technologies that improve efficiency, speed, scalability and profitability. ▪ We have a high appetite for data-driven decision-making and group-wide performance frameworks that enhance operational discipline and transparency. ▪ We have a low appetite for risks that could compromise operational stability, safety, resilience, cybersecurity or compliance with regulatory and industry standards. ▪ We accept moderate, well-managed risks associated with experimentation and change, provided governance, testing and alignment with Group standards are in place.
People & Culture	▪ We have a high appetite for investing in people, leadership development, future skills and new ways of working that strengthen engagement, performance and long-term capability. ▪ We have a high appetite for cultural reinforcement initiatives that strengthen collaboration, agility, inclusiveness and entrepreneurial mindset across the Group. ▪ We have a very low appetite for risks that could harm employee safety, well-being, dignity, or lead to non-compliance with labour laws and ethical standards. ▪ We accept moderate risks linked to organisational change and cultural evolution, provided they are aligned with the Group's values and cultural DNA.
Business Leadership and Regionalisation	▪ We have a high appetite for organic growth, mergers, acquisitions and partnerships that strengthen leadership positions in existing or closely related businesses. ▪ We have a high appetite for scalable regional and international expansion in mastered industries, aligned with a clear regionalisation roadmap. ▪ We have a low appetite for growth initiatives that lack strategic fit, scalability or leadership potential, or that demand disproportionate time and human capital. ▪ We have a very low appetite for investments that undermine long-term value creation, require labour-intensive models, or significantly increase debt at holding level.
Synergies	▪ We have a high appetite for collaboration across businesses to deliver shared growth, cost efficiencies, brand alignment and optimal use of group assets and capabilities. ▪ We have a high appetite for harmonising core processes, systems and standards where this enhances efficiency, consistency and control. ▪ We have a low appetite for synergies that weaken governance or erode individual business strengths. ▪ We have a very low appetite for fragmentation, misalignment or practices that compromise consistency in customer or employee experience across the Group and dilute strategic focus or create operational inefficiencies.

1.5 Enterprise Risk Management framework

The Enterprise Risk Management framework (ERM framework) refers to a set of components that provide the foundation for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Group. The Group's ERM framework is in line with the globally recognised ERM framework released by COSO, 2017 (Committee of Sponsoring Organisations of the Treadway Commission) titled "Enterprise Risk Management – Integrating with Strategy and Performance", as depicted below:

Source: ERM framework advocated by COSO, 2017

1.6 Assurance structure ER Group



The assurance structure identifies internal and external assurance stakeholders responsible for creating, implementing and sustaining ERM initiatives across the Group. The assurance mapping structure aligns individuals, teams, departments with the intent of establishing responsibility and accountability with regard to:

- Integrating ERM into the Group's culture,
- Facilitating and monitoring effective implementation of the ERM framework.

1.7 Roles of key stakeholders

The roles of key stakeholders defined in the ERM function are summarised below. Detailed responsibilities are documented in Annexure 1.

Stakeholder	Composition	Role
Board of Directors	Board of Directors constituted for each listed entity	▪ The Board directs and supervises the management of the business and affairs of the company including to ensure that the company has appropriate risk management / regulatory compliance policies in place. ▪ Promotes a culture of ethical behaviour via dissemination of the Code of Ethics of ER, compliance with the Group's policies and external regulations and risk management.
Risk Committee	NEDs and EDs	▪ Review the Group's procedures to manage or mitigate principal risks and identify emerging risks, to assist in the board's assessment of principal and emerging risks. ▪ Review and assess the company's risk appetite and associated stress testing. ▪ Evaluate the Group's principal risks, to be considered by the board when assessing the Group's prospects.
Audit	INEDs and NEDs	▪ Consider the level of assurance the Audit Committee is getting on the risk management and internal control systems, including internal financial controls, and whether this is enough to help the board in satisfying itself that they are operating effectively.
Risk Management	Head of Risk and supported by a central team of risk professionals	▪ Partner with the clusters in driving the ERM initiative. ▪ Establish and implement processes for risk management across the business and lifecycle of the Group. ▪ Promote risk management culture. ▪ Provide the Risk Committee with updates on key risks across the Group. ▪ Facilitate risk prioritisation and monitoring. ▪ Consolidate and aggregate risks at the Group level.
Internal Audit	Head of Internal Audit (Co-sourced with PwC) and a team of Senior / Internal Auditors.	▪ Provide independent assurance on the design adequacy and operating effectiveness of risk management processes and internal controls across the Group. ▪ Develop a risk-based internal audit plan aligned to the Group's risk register and top risks, approved by the Audit Committee annually. ▪ Report findings and management action plans to the Audit Committee. ▪ Follow up on remediation of identified control gaps. ▪ Include AI systems and automated decision-making processes within the audit scope where these present material risk.
Risk owner	Head of dept, CEOs and Risk Champions	▪ Has the accountability and responsibility to manage a risk.

1.8 Enterprise Risk Management Guideline

The ERM guidelines provide supporting information to assist Management in the execution of the ERM processes.

ERM process is the systematic application of management policies, procedures and practices to the activity of communicating, consulting and establishing the context for ERM in the Group. The ERM process comprising of risk assessment, risk treatment and risk monitoring applies across the organizational lifecycle.

Source: Image generated by AI

1.9 Combined assurance model

Combined assurance model incorporates and optimises all assurance services and functions so that, taken as a whole, these enable an effective control environment; support the integrity of information used for internal decision making by management and its committees.

The purpose of the combined assurance is to create, preserve and realise value through approach and to drive business objectives focussing on our strategic pillars to unleash business opportunities. This is achieved by uniting all lines of defence by breaking down of silos and implementation of one taxonomy across all governance bodies and functions in the Group.

1.10 Lines of defence model

The established lines of defence model facilitates a coordinated and comprehensive approach to providing assurance to the Risk Committee and the Board of Directors. This coordinated approach

ensures effective and efficient risk management across the organisation, reinforcing accountability in roles at every level.

1st line of defence	2nd line of defence	3rd line of defence	4th line of defence
Operational Management	Support functions and Risk Management	Internal audit	External audit and regulators
Manages risks and implements controls	Provides oversight, guidance and support Ensures compliance and effective risk management practices	Provides independent assurance on the effectiveness of risk management and internal controls	Provides financial and regulatory assurance, while regulators enforce laws and provide oversight and guidance

1.11 Risk assessment

Risk assessment comprises of

- Risk identification
- Risk analysis and
- Risk evaluation

Risk assessment is intended to:

- Proactively identify risks considering the external and internal context
- Provide the Group with an improved understanding of risks that can affect achievement of objectives and the possible business impact of risks materialisation.
- Evaluate the design adequacy of existing response systems
- Enable risk prioritization and further treatment

A detailed risk assessment methodology is provided in subsequent sections. Risk assessment shall also consider the velocity of risk — the speed at which a risk could impact the organisation if it materialises — classified as Rapid (within days), Moderate (within weeks) or Slow (over months).

1.12 Risk identification

Risk identification is the mechanism of identifying exposure to uncertainty across the Group, clusters and corporate services. This involves assessment of the external environment within which the Group operates, as well as the internal context of the Group, its clusters and corporate services.

As part of risk identification, a comprehensive list of risks is generated based on events which may prevent, degrade, accelerate or delay the achievement of objectives. The risk causes, source, events, situations or circumstances which could have a material impact on the objectives of the Group and its clusters shall also be identified during this phase.

Risks for each subsidiary and Group shall be documented in individual risk registers. The ownership of these risk registers shall lie with subsidiary and functions; however the Risk Management function shall assist in creating and updating the registers. The format for maintaining risk registers is appended Annexure 2.

1.13Risk analysis

Risk analysis refers to the process followed to comprehend the nature of risk and determine the level of risk. Risk analysis is intended to provide inputs for risk evaluation. Risk analysis shall be performed for each risk identified.

When assessing impact, risk owners shall consider five dimensions:

i. Financial — direct monetary loss;
ii. Operational — disruption to business processes and service delivery;
iii. Reputational — effect on brand and stakeholder confidence;
iv. Legal and Governance — likelihood of sanction or fine; and
v. Strategic — impairment of the Group's long-term objectives.

For AI risks, a sixth dimension applies:

vi. Ethical / Societal — harm arising from biased, opaque or unsafe AI outputs affecting customers, employees or third parties. AI systems must operate with an appropriate level of transparency to ensure that users and stakeholders understand how Artificial Intelligence is used within the organization.

1.14 Consolidate risks

Each subsidiary shall arrive at a number of top risks for their respective entities which shall then be prioritized at the subsidiary's level. Similarly, top risks for all subsidiaries shall be consolidated and prioritized to arrive at a portfolio of top risks for the Group.

In order to visually depict the prioritization, a "heat map" (graphical representation of impact and likelihood) maybe used based on the risk analysis (i.e. Likelihood * Impact) wherein each risk will be plotted on the "heat map" based on its relative likelihood and impact. The placement of the risks on the "heat map" will indicate the risk zone (Critical/High/ Medium/ Low) for each of the respective risks.

A risk report containing the "heat map" and the material risks for the subsidiary shall be prepared and circulated to the respective subsidiaries' senior management and same shall be tabled and presented every quarter to the Risk Committee as appended in Annexure 3.

A five by five matrix shall be used for measuring likelihood and impact. The risk shall be evaluated as:

Risk Measurement: Likelihood * Impact

The risk measurement scale in terms of impact and likelihood has been defined in Annexure 4 – Risk assessment parameters. The risks assessed can be placed on a "heat map" which is a graphical representation of the impact and likelihood.

The overall risk measurement will be assessed as below:

Likelihood * Impact	Risk rating
Score – less than 5	Low
Score – greater than or equal to 5 but less than 15	Medium
Score – greater than or equal to 15 but less than 20	High
Score – greater than or equal to 20	Critical

1.15 Risk treatment

Risk treatment involves selecting one or more options for managing risks, and implementing such action plans. For the purpose of risk treatment, risk owners may consider various options (as indicated below) for risk treatment:

- Avoiding the risk by deciding not to start or continue with the activity giving rise to such risk
- Taking or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood or consequences of risk by instituting new control/ monitoring activities
- Sharing the risk with another party or parties (e.g insurance)
- Putting in place a mechanism to monitor the risk

1.16 Risk monitoring and review

Risk monitoring, review and reporting are critical components of the ERM process. The intent of monitoring and reviewing risks and their respective treatment plans is to:

- Analyse and track events, changes, trends which affect individual risks.
- Ensure that risk treatment mechanisms (Actions plans to be implemented) are effective in design and operation.

Risk monitoring shall be conducted by each subsidiary, for identified risks, in order to track the status of treatment plans.

Risk reviews shall be conducted by the Risk Management function to enable continuity of the ERM process. Risk reviews entail the reassessment of all material risks recorded in the subsidiary's risk registers along with new/ emerging risks to ensure concurrence and relevance of risks and their treatment. Risk reviews will be carried out on a bi-annual basis.

Key Risk Indicators (KRIs):

The Risk Management function shall develop and maintain a KRI framework for the Group's top 10 risks, including AI risk. Each KRI shall specify: the metric tracked; green, amber and red thresholds aligned to appetite tolerances; and the escalation action when thresholds are breached. The KRI dashboard shall be reported to the Risk Committee quarterly.

Trigger-based re-assessment:

A risk re-assessment shall also be triggered by: completion of a significant M&A transaction; entry into a new geographic market; a major regulatory or legislative change (including new AI regulation); a significant adverse risk event within the Group or a peer; or deployment of a material new AI system across the Group.

1.17Managing materialised risks

In the event of a particular risk materializing, it is necessary to have in place a crisis/ incident management procedure for timely and effective management of such events. The incident management procedure is a set of well-coordinated actions aimed at preparing and responding to unpredictable events with adverse consequences. The intention of this plan is to preserve the confidence of internal and external stakeholders in the Group's risk readiness for potentially adverse events. The use of AI within the organization must support productivity and innovation without compromising confidentiality, compliance, or trust.

1.18 Reference

1.19 Documentation

The following documents are generated during the course of the ERM exercise

Document	Description	Owner	Periodicity of review	Format reference
Risk register	Record / log of information about identified risks	Risk Management Department	Bi-annual basis or if there is a material event	Annexure 2
Risk report	A report listing material risks (Identified risks with Inherent Risk rating of High or Critical) intended to inform subsidiary's senior management and Group's Risk Committee regarding the current state of key risks.	Risk owners	Bi-annual basis or if there is a material event	Annexure 3

1.20 Sample risk categories

Risk identified and assessed can arise from multiple categories. Some sample categories are provided below.

Risk category	Definition
Strategic	Potential risk arising from poor business decisions, improper service or offering or limited business analysis
Operational	Potential risk arising from ineffective internal business processes and procedures, people, systems
Financial	Potential risk of cash flows generated not being adequate to meet financial obligations
Market	Potential risk arising from adverse market movements or liquidity constraints
People	Potential risk arising from the Company's inability to attract, retain or properly train qualified individuals
Health and Safety	Potential risk arising from threats or inadequate safeguards to maintain both the well-being of the Company's human capital and the public's safety
Climate and Nature	Potential risk arising from physical climate events, energy transition risks, stranded assets, or ESG rating deterioration affecting access to capital and stakeholder trust.
Legal and Governance	Potential risk arising from legal action, contractual breaches or adverse statutory modifications
Information Technology	Potential risk arising from the failure or inadequacy of information technology
Reputational	Potential reduction to equity value or market share (revenue) arising from negative publicity
Cyber and Data Privacy	Potential risk arising from cyber-attacks, data breaches, ransomware or non-compliance with data protection laws, resulting in financial loss, regulatory sanction or reputational damage.
AI (Artificial Intelligence)	Potential risk arising from the development, deployment or use of AI and machine learning systems across the Group. Managed in accordance with the AI Impact Assessment of ISACA and AI Security Risk Assessment of NIST AI Risk Management Framework (AI RMF 1.0).
Social	Potential risk arising from the organisation's impact on employees, customers, suppliers and communities, including poor labour practices, human rights violations or failure to meet social responsibilities.

1.21 Annexure

Annexure 1: Roles and responsibilities of key stakeholders

This section collates all annexure that have been referred to in this document.

Annexure 1: Roles and responsibilities

A. Board of Directors of ER Group
   - The Board directs and supervises the management of the business and affairs of the company including to ensure that the company has appropriate risk management.
   - Promotes a culture of ethical behaviour via dissemination of the Code of Ethics of ER, compliance with the Group's policies and external regulations and risk management.
   - Reviews risk assessment policies and controls including insurance covers and compliance with legal and regulatory requirements.

Source: ER Board Charter

B. Risk Committee
   - Review the company's procedures to manage or mitigate principal risks and to identify emerging risks, to assist in the board's assessment of principal and emerging risks;
   - Review the company's processes for identifying and assessing sustainability risks and climate change risks;
   - Review and assess the company's risk appetite and associated stress testing;
   - Evaluate the company's principal risks, to be considered by the board when assessing the company's prospects;
   - Review and approve the statements to be included in the annual report concerning internal controls and risk management;
   - Receive reports, as necessary and appropriate, regarding significant new product risk, emerging risks and regulatory matters related to the Committee's authority, duties and responsibilities as set forth in this charter;
   - Help to set the tone and develop a culture of the enterprise vis-à-vis risk, promote open discussion regarding risk, integrate risk management into the organisation's goals and compensation structure, and create a corporate culture such that people at all levels manage risks rather than reflexively avoid or heedlessly take them;
   - Monitor all enterprise risks; in doing so, the Committee recognises the responsibilities delegated to other committees by the board and understands that the other committees may emphasise specific risk monitoring through their respective activities;
   - Review disclosures made in line with sustainability and climate change risks;
   - Oversee workplace health and safety risk management process and reporting as well as Data Protection and Money Laundering processes and controls.
   - In coordination with the Audit Committee, understand how the company's internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs;

- Respond to reports from management so that management understands the importance placed on such reports by the Committee and how the Committee views their content.

Source: Risk Committee Charter

C. Audit Committee
   - Review the company's internal financial controls, that is, the systems established to identify, assess, manage and monitor financial risks.
   - Consider the level of assurance it is getting on the risk management and internal control systems, including internal financial controls, and whether this is enough to help the board in satisfying itself that they are operating effectively.
   - Monitor and review the effectiveness of the company's internal audit function, in the context of the Group's overall risk management system.

Source: Audit Committee Charter

D. Risk Management
   - Establish and maintain the ERM framework, supporting policies, procedures and tools. Partner with clusters and corporate functions to drive ERM implementation.
   - Facilitate the bi-annual risk assessment cycle and consolidate risk registers at Group level.
   - Develop and maintain the KRI framework and dashboard.
   - Co-ordinate the annual AI risk review in accordance with the NIST AI RMF 1.0.
   - Provide the Risk Committee with regular updates on the Group's risk profile.

E. Internal Audit
   - Develop a risk-based internal audit plan aligned to the Group's risk register and top risks, approved by the Audit Committee annually.
   - Provide independent assurance on the design adequacy and operating effectiveness of risk management processes and internal controls.
   - Include AI systems and automated decision-making processes within the audit scope, assessing compliance with the NIST AI RMF 1.0 where material AI systems are in use.
   - Report findings and management action plans to the Audit Committee. Follow up on remediation of identified control gaps.

F. Risk owner
   - Accept accountability for the management of assigned risks.
   - Ensure risk registers for their respective areas are maintained and updated on a timely basis.
   - Design, implement and monitor risk treatment plans and report progress to the Risk Management function.

Annexure 2: Risk register format

Risk identification				Inherent risk			Existing mitigating response				Residual risk			Mitigating action to be implemented			
Risk No	Risk type	Risk title	Risk description	Impact	Likelihood	IR score	First line of defence	Second line of defence	Third line of defence	Fourth line of defence	Impact	Likelihood	RR score	First line of defence	Second line of defence	Third line of defence	Fourth line of defence

Annexure 3: Format risk report

Risk report to Company A

Company A – Top cluster risks

No	Risk type	Description	Residual Risk
STR3	Strategic	Risk A	20
TEC1	Technology	Risk B	16
STR1	Strategic	Risk C	16
STR2	Strategic	Risk D	16
STR5	Strategic	Risk E	16