GraceKennedy Limited Policy	
Policy	**ENTERPRISE RISK MANAGEMENT POLICY**

1. INTRODUCTION

GraceKennedy understands that a changing risk landscape is inherent to its operations and recognizes the need for proactive risk management in achieving its strategic objectives. The purpose of this policy is to outline the approach towards Enterprise Risk Management (ERM) across the Group.

2. DEFINITIONS

"Control" refers to a process, policy, system, practice, resource, or other action that is in place to respond to a risk by either reducing the likelihood or impact of a negative risk or threat; or improving the likelihood or impact of a positive risk or opportunity.

"Enterprise Risk Management (ERM)" refers to the culture, capabilities and practices that are integrated with strategy-setting and performance to comprehensively identify, assess, manage, monitor, and communicate risks across the organization to create, preserve and realize value.

"Impact" refers to the potential outcome or consequence of a risk event on the organization's objectives, operations, financial performance, reputation, or stakeholders.

"Key Risk Indicator (KRI)" refers to a quantifiable or measurable metric that provides an early warning sign of a potential risk event materializing.

"Likelihood" refers to the probability or chance of a risk event occurring within a given timeframe.

"Portfolio view of risks" refers to the holistic assessment and management of all risks across the organization, considering the cumulative severity of individual risks and their interrelationships on overall performance and objectives.

"Risk" is the possibility of an event occurring that could impact the achievement of an objective, either in a negative (threat) or positive (opportunity) way.

"Risk Appetite" refers to the type and level of risk that an organization is willing to accept in pursuit of its strategic objectives.

"Risk Assessment" refers to the process of identifying, analysing, and evaluating risks to determine their potential likelihood and impact.

“Risk Identification” refers to the process of identifying and documenting potential risks that may affect the achievement of the organization’s objectives.

“Risk Management” refers to the coordinated application of policies, procedures, resources, and practices to effectively identify, assess, prioritize, respond to, and monitor risks to minimize threats and while maximizing opportunities.

“Risk Tolerance” refers to the acceptable level of variation in performance that the organization is willing to tolerate in pursuit of strategic objectives.

“Strategic Business Unit (SBU)” means operations within the Group that are managed and reported on as a distinct unit. It may be a company or a division/department/subset of a company.

“Subsidiary” means an entity which is controlled by GraceKennedy Limited.

3. SCOPE

This policy applies to:

3.1. GraceKennedy Limited and its subsidiaries, affiliates, divisions, and departments (collectively referred to as "the Group"), irrespective of their geographical location or business activities.

3.2. Business activities undertaken by the Group, including core operations, strategic initiatives, new ventures, and ongoing projects.

3.3. Types of risks, which includes financial risks, operational risks, strategic risks, and compliance risks.

3.4. Levels of the Group, from the Board of Directors and senior management to individual employees.

4. POLICY STATEMENTS

4.1. **Governance and Culture** shall be a component of GraceKennedy's ERM Framework and lay the foundation for effective risk management by establishing a strong leadership commitment to a risk-aware culture.

4.1.1. Senior management shall actively champion risk management, by integrating it into strategic planning and decision-making to send a clear message throughout the Group about the importance of proactively managing risks.

4.1.2. There shall be a well-defined oversight structure which assigns clear roles and responsibilities for risk management at different levels throughout the

Group to ensure accountability and facilitate effective communication of risks.

4.1.3. Team members shall actively promote a culture that values open communication and rewards responsible risk-taking within defined boundaries to foster a proactive approach to risk management.

4.1.4. A clearly defined risk appetite shall be in place to establish the level of risk that the Group is willing to accept in pursuit of its strategic objectives to ensure that risk management practices support the overall strategy and is aligned to core values.

4.1.5. GraceKennedy shall attract, develop, and retain skilled individuals equipped to identify and manage risks effectively to build risk management capabilities at all levels.

4.2. **Strategy and Objective-Setting** shall be a component of GraceKennedy's ERM Framework and emphasize the integration of risk management with the strategic planning process.

4.2.1. GraceKennedy shall continuously monitor internal and external factors that could impact the Group's risk profile, to include conducting regular risk assessments to identify potential threats and opportunities.

4.2.2. Risk tolerance shall become a guiding principle for evaluating strategic options and making informed decisions.

4.2.3. When evaluating alternative strategies, the Group shall consider the potential impact to ensure that chosen strategies are aligned with both risk appetite and long-term value creation.

4.2.4. Business objectives at all levels shall be established with potential risks in mind by considering the potential impact of risks on achieving these objectives and incorporating risk control strategies as needed.

4.3. **Performance** shall be a component of GraceKennedy's ERM Framework and focus on actively identifying, assessing, prioritizing, and responding to risks throughout the Group.

4.3.1. GraceKennedy shall implement a systematic approach to identifying potential risks that could impact the achievement of strategic objectives, to include various methods such as scenario planning, process mapping, and employee surveys.

4.3.2. Once identified, risks shall be evaluated based on their likelihood of occurring and the potential impact if the risk were to materialize to help prioritize risks and allocate resources for risk response efforts.

4.3.3. Risks shall be prioritized based on their severity in relation to the Group's risk appetite to inform decision-making at all levels, ensuring critical risks are addressed effectively.

4.3.4. Based on the risk assessment, the Group shall select appropriate risk response strategies, whether to accept, avoid, pursue, reduce, share, review business objective or review strategy.

4.3.5. GraceKennedy shall maintain a comprehensive portfolio view of all its risks and consider their interconnectedness and overall severity on the Group's objectives to allow for more effective risk management decisions.

4.4. **Review and Revision** shall be a component of GraceKennedy's ERM Framework and emphasize the importance of regularly reviewing and adapting the ERM program to ensure its effectiveness and adaptability to changing circumstances.

4.4.1. GraceKennedy shall continuously monitor internal and external factors that could significantly impact its strategy and objectives to allow for early identification of emerging risks and timely adjustments to the risk management program.

4.4.2. The Group shall regularly assess its performance and the effectiveness of the ERM program to evaluate whether the implemented risk management practices are adequately in response to identified and emerging risks.

4.4.3. GraceKennedy shall foster a culture of continuous improvement by actively seeking opportunities to enhance the program's effectiveness and address any identified weaknesses based on performance evaluations and changing circumstances.

4.5. **Information, Communication, and Reporting** shall be a component of GraceKennedy's ERM Framework to reinforce effective communication and information sharing through various channels including regular reporting and training.

4.5.1. The Group shall utilize information systems to capture, analyse, and communicate risk-related data effectively to ensure data accuracy, facilitate risk reporting, and support informed decision-making.

4.5.2. Clear communication channels shall be established to facilitate the timely and transparent flow of risk information at all levels across the Group to allow for early identification of issues and foster collaboration in managing risks.

4.5.3. GraceKennedy shall report on key risk, culture, and performance metrics at appropriate levels such as executive, senior management and Board committees within the Group to promote accountability, allow for informed

decision-making by various stakeholders, and maintain a strong risk management culture.

5. ROLES AND RESPONSIBILITIES

5.1. **Board of Directors** shall:

5.1.1. Set the organization's risk tone at the top by establishing a clear risk policy and risk appetite and ensuring effective oversight of the ERM program.

5.1.2. Review and approve the Group's overall risk management and internal controls strategy and major risk management initiatives.

5.1.3. Hold senior management accountable for the implementation and effectiveness of the ERM program.

5.1.4. Receive regular reports on the organization's risk profile, including emerging risks, significant risks to the Group and whether they are being manage appropriately and the performance of the ERM program.

5.1.5. Proactively seek information on emerging risks within the industry and broader environment that could impact the Group.

5.2. **Audit Committee** shall:

5.2.1. Provide oversight of the risk management and internal controls program on behalf of the Board, in accordance with its Terms of Reference.

5.2.2. Review the adequacy of the management of key risk exposures as well as the efficiency and effectiveness of the enterprise risk management program.

5.2.3. Provide an evaluation of the performance of enterprise risk management and internal control framework.

5.3. **Chief Executive Officers (CEOs)**

The Group CEO is ultimately responsible for ensuring that an adequate ERM program is established, implemented, and maintained consistently across the Group and shall:

5.3.1. Demonstrate a strong commitment to risk management through actions and decision-making.

5.3.2. Allocate necessary resources to support the implementation and ongoing development of the ERM program.

5.3.3. Ensure that risk management practices are aligned with the organization's overall strategy and objectives.

5.3.4. Oversee senior management's implementation of the ERM program and hold them accountable for its effectiveness.

5.3.5. Clearly communicate the importance of risk management to all employees and officers of the Group.

5.4. **Chief Risk Officer / Head of Risk** shall:

5.4.1. Lead the development, implementation, and maintenance of the Group's ERM Program including initiatives to raise awareness about risk management and promote a risk aware culture.

5.4.2. Oversee all risk management activities across the Group, including risk and control assessments of strategic objectives, initiatives, new products and services.

5.4.3. Overview the revision of risk documents including policies, procedures, and risk appetite statements. Facilitate communication and collaboration on risk management matters across all levels and departments within the Group.

5.4.4. Provide regular reports to the Group CEO, Executive Committee and Board Committees regarding the Group's risk profile, effectiveness of the ERM program, and any emerging risks.

5.4.5. Advise the Group CEO and the Executive Committee on matters to do with enterprise risk management and program effectiveness.

5.4.6. Develop and implement key performance indicators (KPIs) to track the effectiveness of the ERM program and key risk indicators (KRIs) to monitor and report on key risk exposures, testing and remediation of internal controls.

5.4.7. Benchmark the Group's ERM program against industry best practices and identify opportunities for improvement.

5.5. **Senior Management & Executives** shall:

Have accountability for risk management within the Group and shall:

5.5.1. Embed risk management practices into their respective areas of responsibility, ensuring risk considerations are integrated into decision-making processes.

5.5.2. Identify and manage risks specific to their areas of responsibility, developing and implementing appropriate risk response strategies.

5.5.3. Report identified risks and risk management activities to the Chief Risk Officer or designated risk management personnel.

5.5.4. Integrate risk management performance into employee performance reviews to incentivize proactive risk identification and mitigation.

5.5.5. Communicate the organization's risk management approach and expectations to their respective teams ensuring all employees understand their roles and responsibilities in risk management.

5.5.6. Ensure that there is periodic reporting on the status of enterprise risk management matters at the divisional and SBU level.

5.6. **First Line of Accountability – Strategic Business Unit** shall:

5.6.1. Identify and own risks associated with their daily activities and responsibilities.

5.6.2. Implement and maintain effective risk controls within their areas to manage identified risks.

5.6.3. Escalate significant or emerging risks to the second line for further assessment.

5.6.4. Report incidents and near misses promptly, providing valuable data for risk identification and control strategies.

5.6.5. Complete assigned risk management training programs to gain necessary skills and knowledge to effectively manage risks in their areas.

5.7. **Second Line of Accountability – Support Functions** shall:

5.7.1. Provide expertise and guidance on risk management practices to the first line of defence within their functional areas.

5.7.2. Monitor the effectiveness of risk controls implemented by the first line and report any identified weaknesses.

5.7.3. Develop and maintain risk management policies and procedures specific to functional areas.

5.7.4. Analyse risk data and identify trends to inform risk control strategies and resource allocation.

5.7.5. Conduct risk assessments specific to functional areas to identify potential and emerging treats and opportunities and recommend control strategies.

5.8. **Third Line of Accountability – Assurance Functions** shall:

5.8.1. Review and provide assurance on the appropriateness and effectiveness of major risk response strategies.

5.8.2. Identify any gaps or weaknesses in risk controls implemented by the first and second lines of defence.

5.8.3. Investigate significant risk incidents to understand root causes and recommend preventative measures.

5.8.4. Assess and report on the Group's risk management program and culture and provide recommendations for improvement.

5.8.5. Maintain independence and objectivity in performing assurance activities.

6. BREACH OF POLICY

A breach of this policy may result in disciplinary action including separation from the Company in accordance with the Corrective / Disciplinary Action Policy.

7. POLICY REVIEW

This policy shall be reviewed at least every three (3) years.