

Enterprise Risk Management Policy



VGI Public Company Limited

Effective on 27 May 2021

Reviewed on 25 May 2022

VGI Public Company Limited
Enterprise Risk Management Policy

Policy Information

Policy Name	
Policy Version	
Division Author	
Effective Date	

Document History Table

Policy Version	Effective Date	Reviewer	Approver

VGI Public Company Limited
Enterprise Risk Management Policy

Table of Contents

Terms and Abbreviations 3

1 Introduction..... 5

2 Scope of Enterprise Risk Management Policy 5

3 Objectives of Enterprise Risk Management Policy..... 5

4 Enterprise Risk Management Structure 6

5 Enterprise Risk Management Process 7

6 Roles and Responsibilities 9

7 Policy Exception..... 14

8 Policy Maintenance 14

VGI Public Company Limited

Enterprise Risk Management Policy

Terms and Abbreviations

The following is the list of terms and abbreviations used within this policy.

Terms / Abbreviations	Description
COSO ERM 2017	The Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management 2017.
Emerging Risks	The risks that are unknown and unanticipated that may have a major impact on a company's ability to meet its strategic objectives.
Enterprise Risk Management (ERM)	The culture, capabilities and practices, integrated with strategy-setting and its execution that organizations rely on to manage risk in creating, preserving, and realizing value.
Inherent Risk	The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.
Key Risk Indicators (KRIs)	The metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.
Residual Risk	The risk that remains after risk responses are executed (the net risk or risk after controls).
Risk	The possibility that events will occur and adversely affect the achievement of strategy and business objectives. Risk is measured in terms of impact and likelihood.
Risk Appetite	The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
Risk Culture	The values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose.
Risk Heat Map	The visualization of risks presenting a big picture for the likelihood and impact of entity-wide risks within an organization for decision-making purpose.
Risk Profile	A composite view of the risk assumed at a particular level of the entity, or aspect of the business that positions management to consider the types, severity, and interdependencies of risks, and how they may affect performance relative to the strategy and business objectives.

VGI Public Company Limited
Enterprise Risk Management Policy

Terms / Abbreviations	Description
Risk Response	A set of actions that the Management selects, develops, and implements such as avoiding, accepting, reducing, or sharing risk to align risks with the entity's risk tolerances and risk appetite.
Risk Tolerance	The acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective.
RM	Risk Management
RMC	Risk Management Committee

VGI Public Company Limited

Enterprise Risk Management Policy

1 Introduction

VGI Public Company Limited (hereinafter referred to as “VGI” or “the Company”) recognises the significance and value of Enterprise Risk Management (“ERM”) to manage the risks with good corporate governance principles.

The Enterprise Risk Management Policy (hereinafter referred to as “This Policy or ERM Policy”) establishes the structure for effective ERM for VGI, providing guidance in governance structure, processes, roles and responsibilities.

This Policy is established in line with COSO ERM 2017 to manage the risks and enable all Directors, Executives, and Staff at all levels to effectively manage the risks in a systematic and structured manner within the established risk appetite and risk tolerances and to make business decisions considering associated risks.

2 Scope of Enterprise Risk Management Policy

The scope of this Policy shall be applied to VGI.

3 Objectives of Enterprise Risk Management Policy

The overall objective of this Policy is to provide a documented, structured, appropriate, and sufficient ERM framework for VGI to assign roles and responsibilities, create accountability, and effectively manage the enterprise risks. This Policy:

- a) Recognises that risk is considered in all activities from objective and strategy setting, decision making, and daily operations.
- b) Promotes consistency of methodology, assessment and management processes.
- c) Recognises timely and accurate monitoring, review, communication, reporting of risk, and early warning mechanisms for the effective management of risk occurrences.

4 Enterprise Risk Management Structure

The establishment of a formal risk structure helps to clarify and formalize the accountability, roles and responsibilities among various stakeholders involved in the ERM Process across the Company. This also includes defining risk-related decision-making authorities and involves creating a structure for risk information flows and reporting.

VGI Board of Directors is responsible for oversight of the Policies and assigning the appropriate members to the VGI Risk Management Committee.

VGI Risk Management Committee (hereinafter referred to as “RMC”) is responsible for reviewing the Risk Management Policy and oversight of the effectiveness of the Risk Management.

VGI Audit Committee is responsible for overseeing the assurance over the Risk Management.

VGI Public Company Limited

Enterprise Risk Management Policy

VGI Internal Audit Office is responsible for providing independent assurance over the Risk Management.

Risk Management Working Team consists of RM representatives from each Business Unit. The Working Team is responsible for establishing the Risk Management Policy, facilitating the implementation of the Risk Management, reporting risks to the RMC and monitoring the effectiveness of the Risk Management.

Risk Management Representatives consists of RM working teams within each Business Unit. The representatives are responsible for implementing Risk Management and ensuring that risk assessment and control activities are implemented effectively.

Management and Risk Owners at the Business Unit Level are responsible for identifying, assessing, monitoring and reporting risks and ensuring that controls are effective.

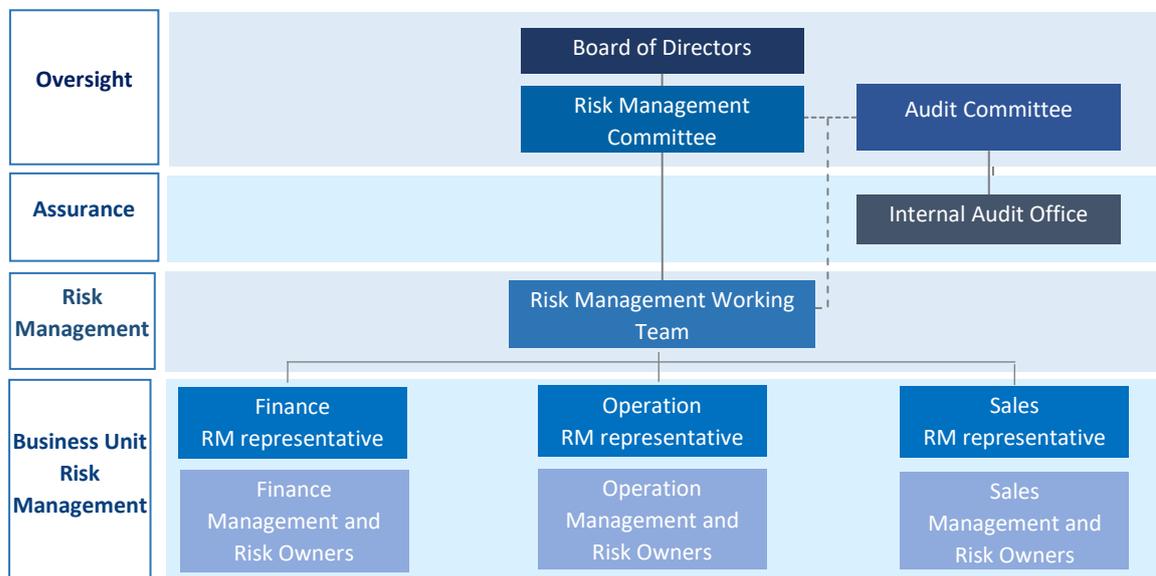


Figure (1) – VGI Risk Management Structure

5 Enterprise Risk Management Process

Enterprise Risk Management is a process to ensure that proper governance and risk culture are in place; significant risks are identified, assessed and managed to be within an acceptable level; and risk monitoring and reporting are effectively implemented.

VGI Public Company Limited

Enterprise Risk Management Policy

The Enterprise Risk Management Process comprises of **FIVE** key activities as follows:

1) Governance and Culture

Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity. Governance and culture cover the following:

- a) Exercise Board Risk Oversight
- b) Establish operating structure
- c) Define desired culture
- d) Demonstrate commitment to core values
- e) Attract, develop and retain capable individuals

2) Strategy and Objective Setting

Enterprise risk management, strategy, and objective setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objective put strategy into practice while serving as a basis for identifying, assessing, and responding to risk. Strategy and objective-setting cover the following:

- a) Analyse business context
- b) Define risk appetite
- c) Evaluate alternative strategies
- d) Formulate business objectives

3) Performance

Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritised by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders. Performance covers the following:

- a) Identify risk
- b) Assess severity of risks
- c) Prioritise risks
- d) Implement risk responses
- e) Develop portfolio view

VGI Public Company Limited

Enterprise Risk Management Policy

4) Review and Revision

By reviewing and entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed. Review and Revision cover the following:

- a) Assess substantial change
- b) Review risk and performance
- c) Pursue improvement in Enterprise Risk Management

5) Information, Communication, and Reporting

Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external. Information, Communication, and Reporting cover the following:

- a) Leverage information and technology
- b) Communicate risk information
- c) Report on risk culture, and performance

The Company considers leveraging information and technology systems to support an effective ERM and communication process. The communication of risk information is significant and must be flown up, down, and across the Company in accordance with the oversight structure (*refer to Figure (1) – VGI Risk Management Structure*) and is summarized as follows:

Risk Reporting	Responsible Person	Frequency	Report to
1. Regular Risk Reporting includes Key Risk Indicators (KRIs), Monitoring Report	BU Risk Owners	Semiannually	Risk Management Working Team
2. Risk Management Report includes KRIs status of the Company	Risk Management Working Team	Semiannually	Risk Management Committee
3. Risk Management Report includes KRIs status of the Company	Risk Management Committee	Semiannually	VGI BOD

VGI Public Company Limited

Enterprise Risk Management Policy

6 Roles and Responsibilities

The key roles and responsibilities of relevant stakeholders related to the Risk Management are summarised as follows:

Business Unit Risk Management	RM Working Team	VGI RMC	VGI BOD
Governance and Culture			
<p>RM Representatives</p> <ol style="list-style-type: none"> Promote risk culture at BU level. Conduct the risk-related training and workshop at the BU level. Provide guidance and facilitate the implementation of the Company Risk Management Policy. <p>Management and Risk Owners</p> <ol style="list-style-type: none"> Promote risk culture within their departments. Participate in risk-related training and workshops at the BU level. Implement and comply with the Risk Management Policy 	<ol style="list-style-type: none"> Promote risk awareness and risk culture to be consistent within the Company. Establish the Risk Management Policy. Align the Risk Management Policy to be consistent within the Company. Communicate the Risk Management Policy to the RM Representatives of each BU. 	<ol style="list-style-type: none"> Encourage risk awareness and risk culture through training and workshops to ensure that all staff levels have enough risk management knowledge. Establish the Risk Management Working Team to assist the RMC in performing its duties. Review the Risk Management Policy to ensure that the policy aligns with the prominent ERM Framework (e.g., ERM COSO). 	<ol style="list-style-type: none"> Set the tone at the top for the desired risk culture including vision, mission and core value of organization. Delegate authorities to the RMC and consider one or more members to have joint membership for both the Audit Committee and Risk Committee for more effective functioning. Approve the Risk Management Policy.

VGI Public Company Limited Enterprise Risk Management Policy

Business Unit Risk Management	RM Working Team	VGI RMC	VGI BOD
Strategic and Objective-Setting			
<p>RM Representatives</p> <p>1. Ensure the alignment of ERM, risk appetite and risk tolerance with each BU strategy and business objectives.</p> <p>Management and Risk Owners</p> <p>1. Set strategy and business objectives that align with the organisation’s mission, vision, and strategies.</p> <p>2. Apply tolerances to specific risks associated with strategy and business objectives.</p>	<p>1. Provide guidance and consultation to each BU in performing ERM process to be aligned with their strategy and business objectives.</p>	<p>1. Provide guidelines for risk consideration in setting strategy and business objectives by Management.</p> <p>2. Provide oversight and hold management accountable for identifying and managing risks to the achievement of objectives.</p> <p>3. Review and approve the Company’s risk appetite and risk tolerance that the Company is willing to accept in pursuit of business objectives.</p>	<p>1. Oversee and advise on strategy and business objectives setting in alignment with risks, vision, mission and culture.</p> <p>2. Establish the overall strategy of the organization and its objectives including understanding the risks associated with the strategy.</p> <p>3. Approve the Company’s risk appetite and risk tolerance that the Company is willing to accept in pursuit of business objectives.</p>
Performance (Risk Assessment)			
<p>RM Representatives</p> <p>1. Facilitate the risk assessment process performed by Management and risk owners.</p> <p>2. Review and advise on the risk assessment process and risk responses processes from risk owners.</p> <p>Management and Risk Owners</p> <p>1. Identify internal and external risk events that impact the Company level and prepare the risk profile, including inherent risks and emerging risks.</p> <p>2. Perform risk assessment and risk prioritisation.</p>	<p>1. Provide guidance and consultation for the risk assessment process to be aligned with ERM Policy and Company’s Risk Taxonomy.</p> <p>2. Consolidate, analyze and validate the risk assessment information prepared by each BU. Determine the risk assessment that impacts at the Company level.</p>	<p>1. Review and approve the Company’s risk profile, risk assessment, and risk response, mitigation plans as proposed by Management.</p> <p>2. Oversee the risk management process on risk identification, risk assessment with respect to their impact and probability of occurrence, risk prioritisation and selection of risk responses in order to ensure that such risks are at an appropriate and acceptable level within the risk appetite and risk tolerance of the Company.</p> <p>3. Challenge Management for their risk assessment where applicable.</p>	<p>1. Approve the Company’s risk profile, risk assessment, and risk response, mitigation plans as proposed by Management.</p>

VGI Public Company Limited
Enterprise Risk Management Policy

Business Unit Risk Management	RM Working Team	VGI RMC	VGI BOD
3. Select appropriate risk responses to manage individual risk, consistent with the risk appetite.			
Review and Revision			
<p>RM Representatives</p> <ol style="list-style-type: none"> Review and ensure the risk profile at the BU level are updated and revision is needed where significant changes or major risks emerge during the year. Monitor the progress of risk mitigation plans at the BU level. Revisit and improve the efficiency and usefulness of existing risk management process at the BU level. <p>Management and Risk Owners</p> <ol style="list-style-type: none"> Consider and monitor risks, including significant changes, or major risks emerging during the year and update risk profiles. Perform the risk mitigation plans and report the results. Implement the risk management improvement process on a regular basis. 	<ol style="list-style-type: none"> Review and ensure the Company risk profile are updated and revision is needed where significant changes or major risks emerge during the year. Monitor the progress of risk mitigation plans at the Company level. Determine the severity of the revision to the risk profile. Revisit and improve the efficiency and usefulness of existing Company risk management process. 	<ol style="list-style-type: none"> Oversee that monitoring activities over risks are functioning at all times. Oversee the progress of significant risk mitigation plans. Review the revision of the Company risk profile. Ensure the continuous improvement of the Company risk management process. 	<ol style="list-style-type: none"> Engage in discussion with the RMC and Management on the existing significant risks faced by the Company in operating its business and change in business context that impact vision, mission, values, strategy and objectives.

VGI Public Company Limited
Enterprise Risk Management Policy

Business Unit Risk Management	RM Working Team	VGI RMC	VGI BOD
Risk Information, Communication, and Reporting			
<p>RM Representatives</p> <ol style="list-style-type: none"> 1. Facilitate the relevant technology to support the ERM process at the BU level. 2. Review and report risks to the RM Working Team. 3. Facilitate the identification of KRIs, monitor the KRIs status and report to the RM Working Team. <p>Management and Risk Owners</p> <ol style="list-style-type: none"> 1. Adopt the relevant technology to support the ERM process. 2. Provide and update regular risk reports (i.e., monthly or quarterly) and progress status to RM Representatives. 3. Identify and report the KRIs to provide early signals of increasing risk exposures in the RM monthly / quarterly meetings. 	<ol style="list-style-type: none"> 1. Introduce and promote the relevant technology to support the ERM process across the Company and to enhance useful information management for decision-making. 2. Identify and report Company’s KRIs to provide early signals of increasing risk exposures to the RMC. 3. Report the KRIs status from all parties across the Company to the RMC. 4. Provide useful risk reports <u>on a regular basis</u> to RMC. 5. Timely escalate significant risks to RMC. 6. Interact and share information or matters regarding enterprise risks with Internal Audit and relevant departments. 	<ol style="list-style-type: none"> 1. Review and approve the relevant technology to support the ERM process to the Board. 2. Review the Company’s risk reports and KRIs status. 3. Provide useful risk reports <u>on a regular basis</u> to the Board. 4. Timely escalate significant risks to the Board. 5. Interact and share information or matters regarding the enterprise risks with the Audit Committee through meetings <u>on a regular basis</u>. 6. Acknowledge the assurance report conducted by the Internal Audit Office <u>on a regular basis</u>. 7. Consider and review the disclosure of information in relation to enterprise risk management in the 56-1 One Report. 	<ol style="list-style-type: none"> 1. Acknowledge regular and significant risks reporting to enable effective decision-making and provide consultation on the action plans. 2. Consider and approve the Company’s risk reports and KRIs status.

VGI Public Company Limited
Enterprise Risk Management Policy

Risk Assurance	
Internal Audit Office	BTSG Audit Committee
<ol style="list-style-type: none"> 1. Review and assess the effectiveness of the risk management processes, as well as the effectiveness and integrity of the business area application for the prescribed risk management processes; 2. Collaborate with the RM Working Team through regular sharing of risk-related information; 3. Develop an internal audit plan considering the enterprise risks; and 4. Review and provide recommendations on the adequacy and effectiveness of the ERM process. 	<ol style="list-style-type: none"> 1. Review the effectiveness and appropriateness of the internal control systems, internal audit system, and Risk Management Policy; 2. Report the opinion of the Risk Management Policy, internal audit plan, internal audit results, fraud, and irregularity in the internal control system to the Board; 3. Ensure that the Internal Audit Office appropriately reviews and assesses the effectiveness of the risk management processes, as well as the effectiveness and integrity of the business area application for the prescribed risk management processes; 4. Interact and share information or matters regarding the enterprise risks with the RMC through meetings <u>on a regular basis</u>; and 5. Review the internal audit plan considering enterprise risks, including fraud risk.

VGI Public Company Limited

Enterprise Risk Management Policy

7 Policy Exception

In situations where Management believes that any aspect of the policy is inappropriate for application, the matter must be referred to the Board of Directors for consideration in advance of any commitment being entered into by the Company.

8 Policy Maintenance

This Policy must be reviewed by the Risk Management Committee on an annual basis and approved by the Board of Directors to ensure the relevance and update of ERM practices. A regular assessment of the ERM process shall be conducted for continuous improvement and alignment with good practices.

This Policy is approved by the Board of Directors on 27 May 2021 and shall take effect immediately.

Approved by

(Chairman of the Board of Directors)