



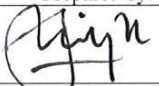
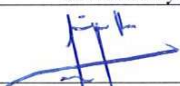


# COMPANY POLICY

## RISK MANAGEMENT POLICY & FRAMEWORK

Doc No: CG-CCC-RMPF-01  
Rev. No: 0  
Date : 14<sup>th</sup> January 2022

Page 1 of 19

# RISK MANAGEMENT POLICY & FRAMEWORK

Prepared by:	Reviewed by:	Reviewed by:	Final Review by:
			
Syed Kamil	Lim Yew Hoe	Mohd Zamzuri Yusoff	Mokhtar Hashim
Head, Corporate Compliance	ED/Chief Financial Officer	Chief Operating Officer	Managing Director
Date: 14/1/2022	Date:	Date:	Date: 25/1/22

*This document is the property of Carimin Group of Companies and shall not be passed to any unauthorized person or party without the written approval of the Managing Director.*

**TABLE OF CONTENTS**

<b><u>SECTION</u></b>	<b><u>DESCRIPTION</u></b>	<b><u>PAGE</u></b>
1.0	ABBREVIATIONS & DEFINITIONS	3
2.0	PURPOSE	4
3.0	SCOPE	4
4.0	REFERENCES	4
5.0	POLICY STATEMENT	5
6.0	RISK MANAGEMENT PRINCIPLES	6
7.0	RISK GOVERNANCE & STRUCTURE	7
8.0	RISK MANAGEMENT FRAMEWORK	8
9.0	ROLES & RESPONSIBILITIES	11
10.0	RISK MANAGEMENT STRATEGY	13
11.0	RISK MANAGEMENT PROCESS & PLAN	14
12.0	RISK CLASSES, TYPES & CATEGORIES	15
13.0	RISK ASSESSMENT	16
14.0	RISK TREATMENT	18
15.0	RISK REGISTERS	18
16.0	RISK APPETITE	18
17.0	RISK REPORTING	19
18.0	BOARD APPROVAL	19

## 1.0 ABBREVIATIONS & DEFINITIONS

**AC** – Audit Committee

**BOD** – Board of Directors

**CCRM** – Corporate Compliance & Risk Management Department

**COSO** – the Committee of Sponsoring Organizations of the Treadway Commission

**Control** – measure that is modifying risk.

**Company** - Carimin Petroleum Berhad and its subsidiaries

**Employee** – any employee of the Company and shall include contract personnel, temporary staff, trainees and interns.

**ERM** – Enterprise Risk Management

**CEO** – Chief Executive Officer of the Company

**COO** – Chief Operating Officer of the Company

**HOD** - Head of Department

**HRD** - Human Resource Department

**IIA** – Institute of Internal Auditors

**Inherent Risk** – the risk level without any controls or that is taken as natural

**ISO** – International Organization for Standardization

**LOD** – Line of Defense

**MACC** – Malaysian Anti-Corruption Commission, also known as SPRM

**Management** – immediate supervisors, HODs, Head of Business Units/Subsidiaries and the MD

**MCCG** – Malaysian Code on Corporate Governance

**MD** - Managing Director of the Company

**MS** – Malaysian Standard

**PIC** – Person-in-charge

**PN** – Practice Note

**Residual risk** – the remaining risk level after a risk has been treated with controls

**Risk** – effect on uncertainty on objectives. It can be positive and/or negative.

**Risk appetite** – amount and type of risk that an organization is willing to pursue or retain

**Risk attitude** – organization’s approach to assess and eventually pursue, retain, take or turn away from risk

**Risk management** – coordinated activities to direct and control an organization with regard to risk.

**Risk matrix** – tool for ranking and displaying risks by defining ranges for the consequence and likelihood

**RMC** – Risk Management Committee

**RMWC** – Risk Management Working Committee

**Risk perception** – stakeholder’s view on a risk.

**SOP** – Standard Operating Procedure

**TOR** – Terms of Reference

## **2.0 PURPOSE**

The purpose of this document is to provide guidance on Risk Management in the Company. It includes Company’s Policy and the necessary Framework for managing risks throughout the Company in an integrated manner, with the full commitment of the Board and Management.

The Framework purpose shall be in alignment with the description as provided in ISO 31000:2018 Section 5. Framework – “The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions.”

## **3.0 SCOPE**

This Policy and Framework shall apply to the entire Company, its Directors, Management and employees; and covers how risk management and compliance activities are implemented.

## **4.0 REFERENCES**

This document shall be read and applied in conjunction with the following laws, regulations, policies, SOPs, guidelines and standards.

### **4.1 Relevant legal and regulatory requirements:**

- a) Companies Act 2016 (Act 777)
- b) Malaysian Code on Corporate Governance (MCCG) – Principle B: Effective Audit And Risk Management

- c) Listing Requirements Paragraph 15.26 (b) – refer to PN 9
- d) Bursa Malaysia Practice Note 9 (PN 9) – Risk Management And Internal Control, Corporate Governance And Sustainability Statement
- e) Statement on Risk Management & Internal Control – Guidelines for Directors of Listed Issuers
- f) MACC Guidelines on Adequate Procedures - Pursuant to Subsection [5] of Section 17A under the Malaysian Anti-Corruption Commission Act 2009 Act 694

**4.2 Company Charters, Terms of Reference, Policies and Procedures:**

- a) Board Charter
- b) Terms of Reference (TOR) of Risk Management Committee (RMC)
- c) Internal Auditors Assessment Policy - Audit Committee (AC)
- d) Carimin Risk Management Booklet

**4.3 Standards & Guidelines**

- a) MS ISO 31000:2020 Risk management - Guidelines (First revision) (identical to ISO 31000:2018 – Risk Management – Guidelines)
- b) MS ISO GUIDE 73:2010 Risk Management – Vocabulary (identical to ISO GUIDE 73:2009 Risk Management – Vocabulary)
- c) The Institute of Internal Auditors (IIA) Position Paper: The Three Lines of Defense in Effective Risk Management and Control (January 2013)
- d) The IIA’s Three Lines Model – An Update of the Three Lines of Defense (July 2020)
- e) The Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Enterprise Risk Management: Integrating with Strategy and Performance.
- f) COSO – Enterprise Risk Management: Applying enterprise risk management to environmental, social and governance-related risks
- g) Institute of Risk Management (IRM) – A Risk Practitioners Guide to ISO 31000:2018
- h) IRM – A Risk Practitioners Guide to the COSO ERM Frameworks

**5.0 POLICY STATEMENT**

Company recognizes that management of risks is one of the essential components of excellent corporate governance.

For continued growth and success, we will conduct our business activities and pursue our objectives in a sustainable and ethical manner by incorporating and embedding risk management into all functions and activities as necessary and in an appropriate manner.

Our Risk Management will enhance our business through the creation and protection of value by having a proper Governance structure, clarity in responsibilities and systematic customized processes within a **Risk Management Framework (RMF)**.

Through a cohesive, prudent and well-coordinated Enterprise Risk Management (ERM), we will be able to identify and manage the various risks elements. Our ERM will be based on international standards and guidelines including **ISO 31000, IIA and COSO**.

Our ERM will enable us to achieve the following:

- (a) A sustainable, safe and healthy work environment.
- (b) Enhanced business performance by identifying and managing both threats and opportunities.
- (c) Clear communication of risks throughout the Group.
- (d) Protection of our reputation, brand and relationship with all stakeholders.

We will provide the necessary resources to ensure the success of our ERM and that everyone in the Group is responsible for the implementation of this Policy and Framework.

The Framework shall be regularly reviewed and continually improved. We shall actively implement a continual improvement approach to risk management and compliance.

## **6.0 RISK MANAGEMENT PRINCIPLES**

Our ERM shall be based on the principles indicated in MS ISO 31000:2020 (Clause 4). These are as follows:

- (a) **Integrated** – whereby Risk Management is an integral part of all our activities.
- (b) **Structured and comprehensive** – this will enable our ERM to be systematic and produce consistent results.
- (c) **Customized** – all our ERM activities will be designed and implemented according to our needs and the risks we face from external and internal sources.
- (d) **Inclusive** -our ERM involves various stakeholders so that a variety of views and perceptions or perspectives can be considered.
- (e) **Dynamic** – this is necessary as threats and opportunities can occur quickly due to the constant change happening, both externally and internally.
- (f) **Best available information** – this will make our decision-making better.
- (g) **Human and cultural factors** – these play an important role in successfully implementing our ERM. We will need to include human behaviour and motivations into our risk management.
- (h) **Continual improvement** – our environment is in constant change and flux, therefore we will need to continually improve through learning and experience. It is an iterative process.

## 7.0 RISK GOVERNANCE & STRUCTURE

Carimin's Risk Governance is designed to apply the principles of good ERM as outlined earlier in Section 6 to ensure that risk levels are within the approved and acceptable limits. This will assure the Group's long-term sustainability.

Our Risk Governance is guided by **COSO's Enterprise Risk Management** strategic concepts, while the structure is based on the **IIA's Three Lines model** (previously known as The Three Lines of Defense or LOD).

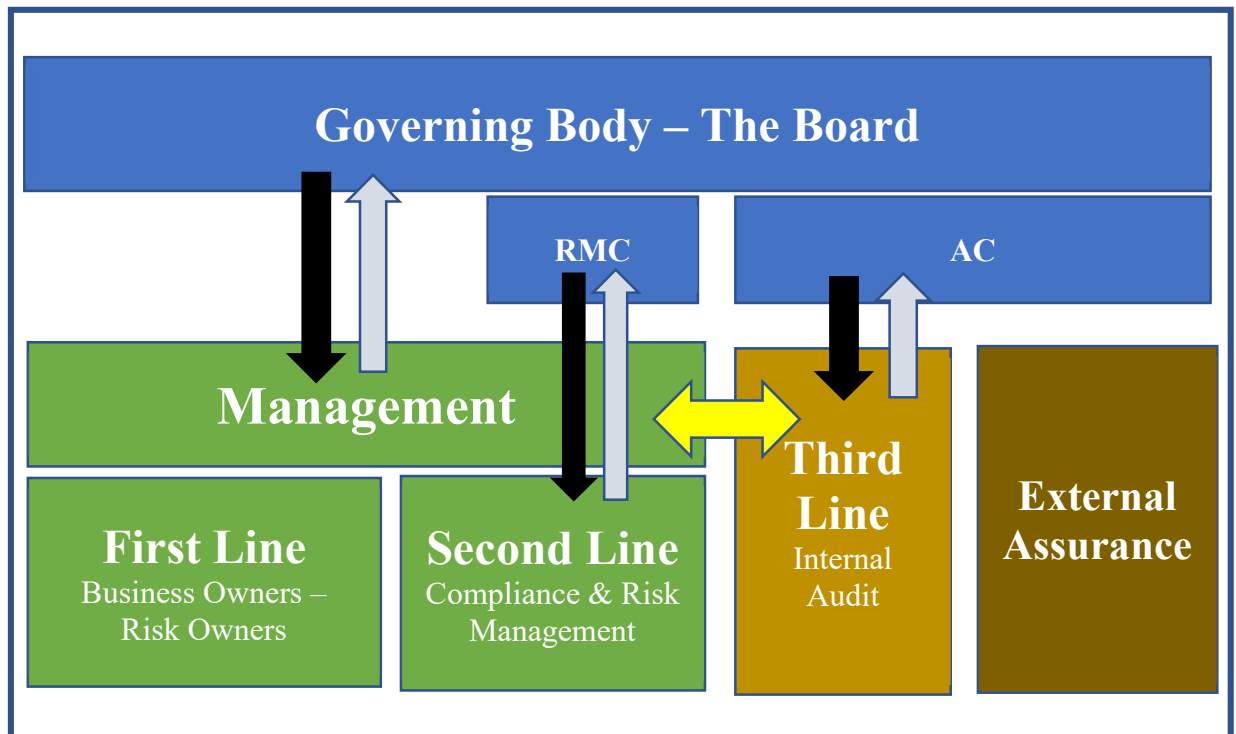
For Carimin Group, the **Three Lines** are:

- (a) **First Line** – the frontliners who actually provides products or services to clients. They are the **risk owners**. They are responsible for managing the risks.
- (b) **Second Line** – these are the functions that provide expertise to support the First Line and monitor risk-related matters. They also ensure that the First Line functions are in compliance and that risks are being managed properly. These are the **Compliance & Control** and **Risk Management** functions.
- (c) **Third Line** – this provides independent and objective assurance as well as advice on the adequacy and effectiveness of governance and risk management. **Internal Audit** provides this function.

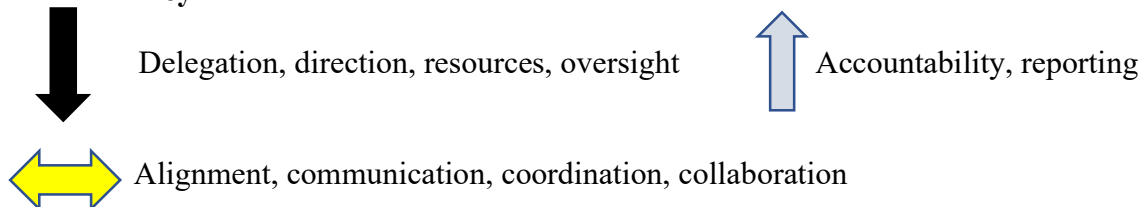
**The Board** being the governing body, together with the **Risk Management Committee (RMC)**, ensures that the above structure and processes are in place; and that they are aligned with the interests of stakeholders.

The structure is as shown below in *Figure 1*.

*Figure 1 – Risk Governance & Structure (Based on IIA Three LOD Model)*



**Key:**



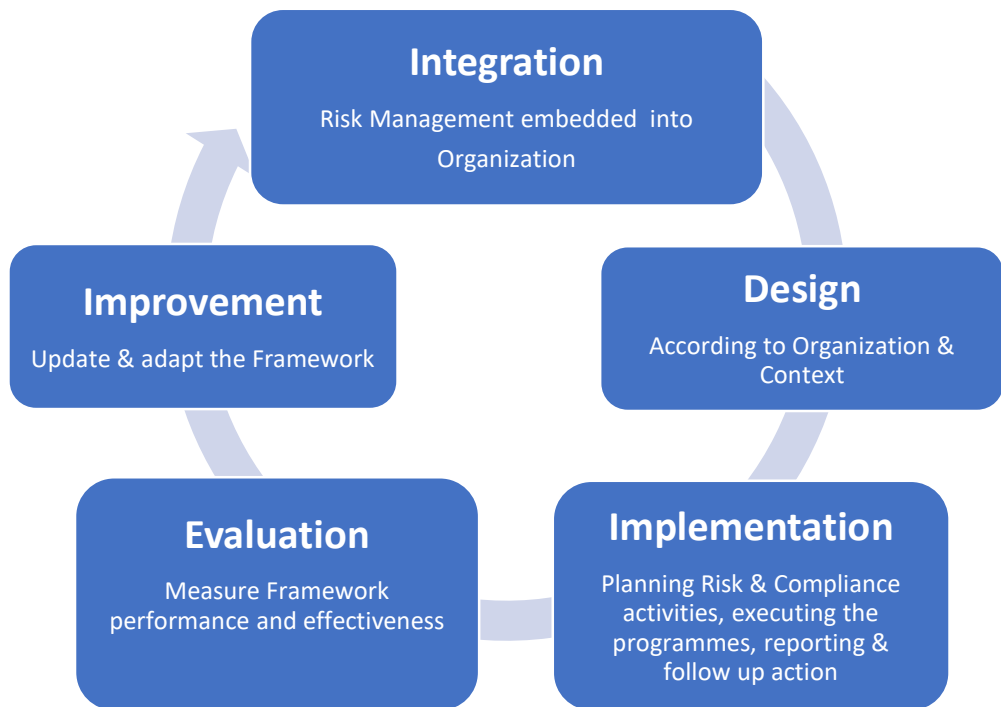
## 8.0 RISK MANAGEMENT FRAMEWORK

A framework specifically for the Company is to be guided by Clause 5 – Framework of ISO 31000 whereby a framework is developed based on integrating, designing, implementing and improving risk management. All these require the support and commitment from stakeholders, particularly senior management.

*Figure 2* shows our Framework development process.



*Figure 2 – Framework Development Process (Based on MS ISO31000:2020)*



Company shall pursue its corporate business objectives in a sustainable and ethical manner, in compliance with all statutory and legal obligations. To enable this, we have adopted a **Risk Management Framework** (the Framework) as illustrated in the diagram *Figure 3* below.

*Figure 3 – Carimin Risk Management Framework*



The key components of our Framework are:

- (a) **Board approved policies and framework** – this provides the foundation for Risk Management throughout the organization and establishes the strategy, objectives and outlines the required processes / practices.
- (b) **Clearly documented roles and responsibilities** – this covers all the committees and the Executive or Management functions, the Operational positions of the First LOD; the Compliance and Risk Management functions of the Second LOD; and Internal Audit being the Third LOD.
- (c) **Risk Management Processes and Methodologies** – this is the implementation aspect of Risk Management and will be consistent with industry standards and best practices of the time.
- (d) **Monitoring, Evaluation and Reporting** – to ensure that Risk Managing is being implemented effectively, Compliance and Internal Audit oversight and assurance functions are required. Compliance & Internal Audit plans, proper and systematic communications together with escalation processes for compliance reporting and whistleblowing/complaints handling are necessary.

In line with the Standards and our Policy Statement, the components shall be regularly reviewed and continually improved.

## 9.0 ROLES AND RESPONSIBILITIES

The table below shows the responsibilities of every entity or person in the organization with respect to Risk Management.

No	Entity / Position	Responsibilities
1	Board of Directors	<ul style="list-style-type: none"> <li>As per the Board Charter</li> <li>Overall corporate governance, reviewing the risk management process and internal control systems to minimize the downside risk for the Company</li> <li>To approve Risk Management Policy and Risk Management Framework (RMF)</li> <li>To establish a Risk Management Committee</li> </ul>
2	Risk Management Committee (RMC)	<ul style="list-style-type: none"> <li>As per the Terms of Reference (TOR) of the RMC</li> <li>Oversee the implementation of policies and RMF of the Company</li> <li>To regularly review the adequacy and effectiveness of risk policies and the RMF</li> <li>Ensure that Management maintains sound system of risk management and internal controls</li> <li>To determine the nature and extent of significant risks which the Company is willing to take</li> <li>To recommend appetite for risk and policy for risk management</li> <li>To meet at least once a year</li> </ul>
3	Managing Director	<ul style="list-style-type: none"> <li>Overseeing the implementation and compliance to this Policy and Framework by the Group</li> </ul>
4	Chief Executive Officer (CEO)	<ul style="list-style-type: none"> <li>Provide leadership in the management of Risks</li> <li>Accountable for the overall implementation and compliance by the Group</li> <li>Monitor and report to the RMC and the Board, as necessary</li> </ul>

No	Entity / Position	Responsibilities
5	Chief Operating Officer (COO)	<ul style="list-style-type: none"> <li>• Responsible for the implementation and compliance by Risk Owners</li> <li>• Lead in enforcing the Framework</li> <li>• Report any incidents or material risk mitigation failures</li> <li>• Take follow up action on risk exposures or failures</li> </ul>
6	Corporate Compliance & Risk Management Department (CCRM)	<ul style="list-style-type: none"> <li>• To perform the annual ERM assessments and report to the Board and Management on the Risk Profile</li> <li>• To update and maintain the Risk Registers</li> <li>• To perform any Risk Management related works as required by Management or RMC</li> <li>• To provide advice on Risk Management</li> <li>• To ensure compliance to Policy and Framework</li> <li>• To maintain breach register</li> <li>• To manage and report whistleblowing cases</li> <li>• To monitor, evaluate, advise and recommend to Management, RMC, AC and the Board on Compliance &amp; Risk Management Matters</li> </ul>
7	Risk Management Working Committee (Members are COO and risk owners HODs)	<ul style="list-style-type: none"> <li>• To monitor and track Risk Management matters</li> <li>• To coordinate with Risk Owners</li> <li>• To discuss and act on risk mitigation</li> <li>• To foster and build a culture where risks are identified and managed properly</li> <li>• To meet at least once every quarter</li> </ul>
8	Risk Owners	<ul style="list-style-type: none"> <li>• To identify all risks associated with their areas of operations</li> <li>• To own and manage the risks identified</li> <li>• Responsible for the implementation of operational procedures and controls which have been put into place to treat or mitigate the risks</li> <li>• To communicate with staff on risk matters</li> <li>• To review risk reports generated by risk champions or coordinators</li> <li>• To escalate risk issues and make recommendations on how to treat the risks or improve on existing SOPs and controls to RMWC and Compliance/Risk Managers</li> </ul>

No	Entity / Position	Responsibilities
9	Risk Champions / Coordinators	<ul style="list-style-type: none"> <li>To submit reports on Risk matters</li> <li>To highlight risk issues to Risk Owners and Compliance/Risk Managers</li> <li>To help promote risk awareness in the department</li> </ul>
10	Internal Audit Consultant	<ul style="list-style-type: none"> <li>To check on compliance by 1<sup>st</sup> LOD and management of oversight by 2<sup>nd</sup> LOD</li> <li>To check on effectiveness of controls</li> <li>To evaluate the risk management systems and functions</li> <li>To perform risk-based audits</li> </ul>
11	Other employees	<ul style="list-style-type: none"> <li>To be aware of risk matters</li> <li>To comply with all policies and procedures</li> <li>To highlight any gaps or issues to Management or to Compliance/Risk Managers</li> </ul>
12	Contractors/Suppliers	<ul style="list-style-type: none"> <li>To comply with the Company's policies &amp; procedures</li> </ul>

## 10.0 RISK MANAGEMENT STRATEGY

Our strategy to ensure a robust and sustainable risk management is as follows:

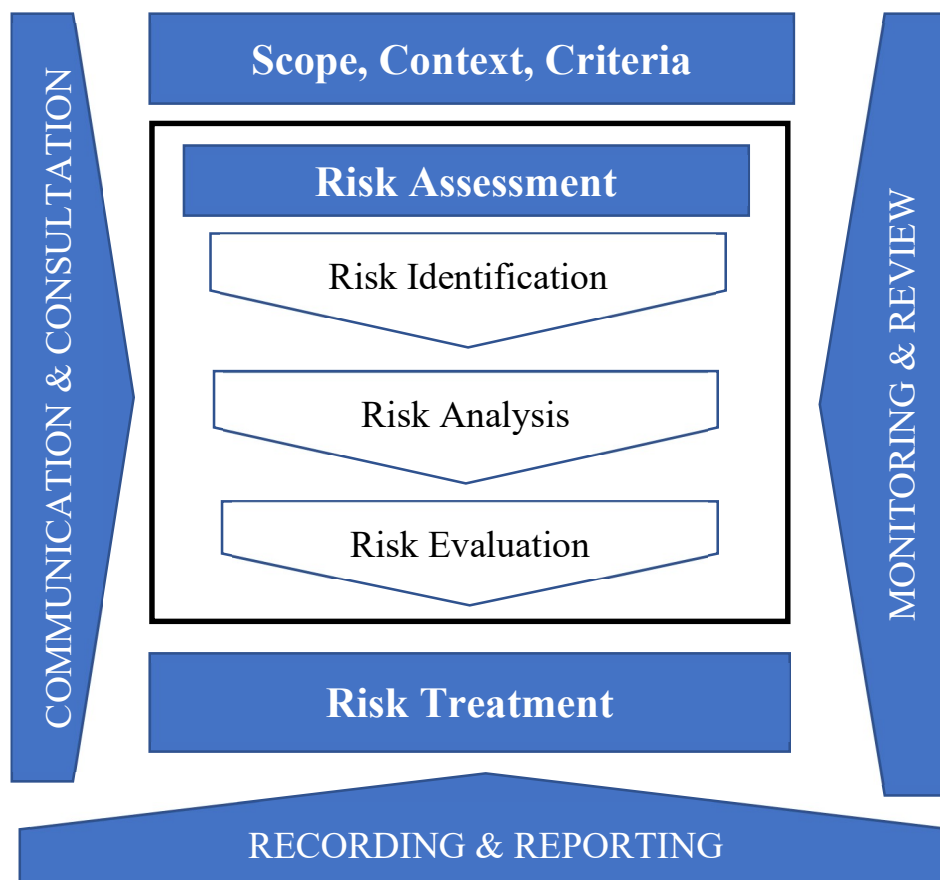
- To build and nurture a strong **risk culture** which encompasses individual and corporate values, attitudes, competencies and behaviour committed towards good governance and risk management. We will work in partnership with HR Department (HRD) on building this culture.
- To **link** our business strategies and operations with good risk management concepts and practices especially for new undertakings, projects or ventures.
- To have strong Board and Management **commitment** on management of risks, thus ensuring the right tone from the top.
- To create **awareness** of risk management concepts, processes and programs throughout the Group. This will be done through training and communications.
- To enhance risk management **capabilities** through training and building systems.
- To develop a **learning** organization which quickly adapt and adjust from past experience and in anticipation of current and also future trends.

## 11.0 RISK MANAGEMENT PROCESS & PLAN

Our risk management process follows the ISO 31000 concept i.e. the systematic application of policies, procedures and practices.

The process involves communications & consultation; establishing the context, assessing, treating, monitoring, reviewing, recording and reporting risks. **Figure 4** below illustrates this process.

**Figure 4 – Risk Management Process (Based on MS ISO 31000:2020)**



The Company shall conduct the following risk management activities:

No	Activity	PIC/Department
1	ERM Assessment – annually	CCRM
2	Project Risk & other risk assessments – as necessary	Project Director / Manager
3	Corruption Risk Assessment – at least once every 3 years, or whenever necessary, refer to MACC Guidelines	CCRM
4	Safety & Environmental Risk Assessment – every year, or whenever necessary	HSE Department
5	Control Reviews – every 3 years or whenever necessary	CCRM
6	Control Self-Assessment (CSA) – risk based, whenever necessary	Every Department
7	Maintain Corporate Risk Registers & Risk Profile	CCRM
8	Maintain Project Risk Registers	Project Director / Manager
9	Maintain Operations Risk Registers	COO
10	Communications & Training Programs	CCRM / HRD

## 12.0 RISK CLASSES, TYPES & CATEGORIES

### 12.1 Classes of Risks

We view risks as being made up of two classes. These are:

- (a) **External Risks** – These are risks which are beyond our control such as geopolitical risks, environmental risks and global market risks.
- (b) **Internal Risks** – These are risks which are within our business activities and which we have control over. These include operational risks, financial risks and product or services risks.

### 12.2 Types of Risks

Risks can be described as two types – inherent and residual. These are defined as follows:

(a) **Inherent Risk** – the risk level which is natural or raw, without any risk treatment applied.

(b) **Residual Risk** – the risk level which remains after treatment by applying controls

When faced with a particular risk, we need to manage and treat the risks accordingly with an objective of reducing the risk level. This treatment process is shown in **Figure 5** below.

**Figure 5 – Risk Treatment**



### 12.3 Categories of Risks

For Carimin Group, risks are categorized as follows:

- (a) External
- (b) Regulatory
- (c) Legal
- (d) Corporate Governance
- (e) Financial
- (f) Operations
- (g) Products & Services
- (h) Customer
- (i) Human Capital
- (j) Suppliers

## 13.0 RISK ASSESSMENT

As per Figure 4 – Risk Management Process, we will perform risk assessments according to the following methodology:



**(a) Risk Identification – What Might Happen, How, When and Why?**

Risk identification is to be performed continually for existing processes and business operations, while for new services and projects or changes to current business set up, this is to be carried out prior to implementation.

Methods of identifying risks include

- i. Consultation with industry or subject matter experts
- ii. Risk Workshops
- iii. PESTLE / SWOT Analyses
- iv. Risk Assessment Questionnaires
- v. Surveys / Interviews
- vi. Internal Audits
- vii. Historical data of risk events – within the company and the industry

**(b) Risk Analysis – What is the Likelihood and Consequence?**

Following risk identification, the risks are classified accordingly as per Section 12.

Each risk shall be analyzed to develop an understanding of the risk, its likelihood, the impact and consequences on our business and operations should it occur.

The analysis will provide the inherent risk in terms of its inherent likelihood and impact. This can then be used to provide us with its inherent risk rating. These are then used for risk profiling.

Existing controls are then taken into consideration and the residual risk level is determined.

Risk analysis shall use a risk matrix for likelihood and impact to indicate the risk level.

Risks can then be compared and prioritized.

**(c) Risk Evaluation – Which Risks to Avoid, Accept, Mitigate or Transfer?**

A risk evaluation shall be conducted to determine whether to avoid, accept, mitigate or transfer a risk based on the Company's approved Risk Appetite, corporate objectives, company policies, legislation and regulations

#### 14.0 RISK TREATMENT

Whenever the residual risk after applying existing controls is still unacceptable, then the risk needs further treatment to reduce the level of risk so that it is within the acceptable tolerance levels.

The Risk Owner shall propose a treatment plan which outlines the actions to be taken to further mitigate the risk. The approved treatment plan will be then be implemented and the results monitored. The resulting risk level is checked to ensure that residual risk has fallen within the acceptable limits.

#### 15.0 RISK REGISTERS

We shall maintain the relevant Risk Registers, including but not limited to the following:

No	Risk Register Type	PIC/Department
1	Enterprise Risk Register	CCRM
2	Corruption Risk Register	CCRM
3	Operations Risk Register	COO
4	Safety & Environmental Risk Register	HSE Manager
5	Project Risk Register – project specific	Project Director / Manager or Business Development

The risk registers will be maintained and updated by the department or personnel specifically assigned the role. All registers shall be provided to CCRM for review and record purposes.

The RMC will receive reports regarding these registers and be advised of any material changes.

#### 16.0 RISK APPETITE

A risk appetite shall be proposed by Management to the RMC. On acceptance by RMC, this will be recommended by the RMC to the Company's Board for consideration and adoption.

The Board approved risk appetite shall be made known to Management. The Company shall operate within the boundaries of the risk appetite.

The RMC shall review the risk appetite regularly to ensure that it remains relevant according to the Group's activities, the size of undertakings and the business environment.

Should the risk appetite limits be breached, risk management controls and actions shall be taken to bring back the exposure within the approved acceptable limits, except those undertakings which have been approved by the Board and where the risks have been noted by the Board.

### **17.0 RISK REPORTING**

Risk registers, profiles and risk management related reports shall be prepared by CCRM and other departments which have been assigned the responsibility.

The registers, profiles and reports shall be reviewed by Management and then submitted to the RMC as per an agreed schedule, or upon request.

The ERM Report shall be submitted annually to the RMC.

Breaches of risk protocols or risk appetite and control failures shall also be reported by CCRM to Management and RMC accordingly.

### **18.0 BOARD APPROVAL**

This Policy and Framework was reviewed and approved by the Board of Directors of the Company on 25<sup>th</sup> November, 2021.