



YINSON HOLDINGS BERHAD

Enterprise Risk Management (ERM) Policy Statement & Framework

08	01/03/2024	Issued for implementation	SCWY	AGAS	BOARD
Rev No.	Date	Reason for Issue	Prepared By	Checked By	Approved By

Document Classification: Proprietary

Document Title:	Enterprise Risk Management (ERM) Policy Statement & Framework			
Document No:	YHB-RC-CG-PP-0004			
Process:	Governance, Risk Management & Compliance	Applicable To:	YINSON Group of Companies	
Revision No:	08	Effective Date:	31 March 2024	



Title : Enterprise Risk Management (ERM) Policy Statement & Framework
Revision : 08
Document No : YHB-RC-CG-PP-0004
Date : 1-Mac-2024

TABLE OF CONTENTS

SECTION 1	PURPOSE
	1.1 Scope
SECTION 2	DOCUMENT OWNERSHIP
SECTION 3	ABBREVIATIONS AND DEFINITIONS
SECTION 4	ENTERPRISE RISK MANAGEMENT FRAMEWORK ARCHITECTURE
SECTION 5	ERM POLICY STATEMENT & FRAMEWORK EXECUTIVE SUMMARY
	5.1 Enterprise Risk Management Policy Statement of Yinson Group
	5.2 Risk Appetite and Tolerance
SECTION 6	RISK MANAGEMENT SCOPE
	6.1 Strategic Risk Management
	6.2 Corporate Risk Profile based on Business Function
	6.3 Strategic Investment, Key Business Activities, and New Projects/Segment
SECTION 7	GOVERNANCE OVERSIGHT STRUCTURE
SECTION 8	ROLES AND RESPONSIBILITIES
SECTION 9	ENTERPRISE RISK MANAGEMENT PROCESS
	9.1 Establishing Context
	9.2 Risk Control Self-Assessment (“RCSA”)
	9.3 Risk Treatment
	9.4 Risk Monitoring and Review
	9.5 Risk Retirement
	9.6 Risk Reporting
	9.7 Communication and Consultation
SECTION 10	EMERGING RISK
	10.1 Identification of Emerging Risk
SECTION 11	KEY RISK INDICATOR (“KRI”)
	11.1 KRI Requirements
	11.2 KRI Process
SECTION 12	SCENARIO PLANNING
SECTION 13	ENTERPRISE RISK MANAGEMENT ENABLERS
	13.1 Risk Culture
	13.2 Trainings and Communications
	13.3 Monitor and Continual Improvements
SECTION 14	APPENDICES
	14.1 Climate Risk Assessment
	14.2 Risk Likelihood Description
	14.3 Detailed Risk Impact Rating for Financial Parameters
	14.4 Detailed Risk Impact Rating for Non-Financial Parameters
	14.5 Risk Matrix Descriptions
	14.6 List of Acts and Legal References



Revision Details

Rev. No.	Section	Details
08	Section 4.0 ERM Framework Architecture	<u>Enhancement to the overall ERM Framework Architecture</u> <ul style="list-style-type: none"> Inclusion of three lines of defense description Update of business unit's Advisory Board role in the framework
	Section 5.0 ERM Policy Statement & Framework Executive Summary	<u>Enhancement to the policy statement and risk appetite</u> <ul style="list-style-type: none"> Revision of the ERM Policy Statement of Yinson Group to be aligned with Board Charter Revision of Risk Appetite Statement to be updated and aligned with Yinson's strategic direction
	Section 6.0 Risk Management Scope	<u>Enhancement to the overall scope of risk management in Yinson</u> <ul style="list-style-type: none"> Enhancement to the risk category descriptions Revision of ERM process for strategic investment, key business activities and new projects/segment following the decentralisation
	Section 7.0 ERM Governance Structure	<u>Revision of risk reporting line within ERM Governance Structure</u> <ul style="list-style-type: none"> Update of business unit's Advisory Board role Revision of the risk reporting line for business units following the decentralisation
	Section 8.0 Roles and Responsibilities	<u>Update of the roles and responsibilities within ERM Governance Structure</u> <ul style="list-style-type: none"> Inclusion of business unit's Advisory Board role and responsibility Update of responsibility descriptions to be aligned with respective Term of Reference ("TOR")/ Charter
	Section 9.0 ERM Process	<u>Enhancement to the overall ERM Process</u> <ul style="list-style-type: none"> Enhancement to the existing ERM processes based on current gaps Revision of residual risk rating criteria Inclusion of risk retirement process Inclusion of immediate risk escalation process
	Section 10.0 Emerging Risk	<u>Newly added section of Emerging Risk</u> <ul style="list-style-type: none"> Inclusion of detailed process to identify emerging risks
	Section 11.0 Key Risk Indicator	<u>Newly added section of Key Risk Indicator ("KRI")</u> <ul style="list-style-type: none"> Inclusion of KRI requirements and process
	Section 12.0 Scenario Planning	<u>Newly added section of Scenario Planning</u> <ul style="list-style-type: none"> Inclusion of guidelines for Scenario Planning
	Section 14.0 Appendix	<u>Enhancement to the risk parameters</u> <ul style="list-style-type: none"> Enhancement to the detailed risk impact rating for non-financial parameters
	All	<u>Enhancement and standardisation of format, structure and wordings within the Policy</u> Changes made includes: <ul style="list-style-type: none"> Format of the document Update of business unit, committee, and department name



1.0 Purpose

The Enterprise Risk Management (“ERM”) Policy Statement & Framework is a documented and established foundation for the enterprise-wide risk management approach in Yinson Holdings Berhad (also known within the document as “Yinson” or “the Group”). The objective of the framework is to:

- Define and communicate the risk appetites and strategies of the Group;
- Define the scope and coverage of the ERM Framework;
- Establish and define the governance structure, roles and responsibilities; and
- Articulate the overall ERM process and approach.

The ERM Framework is developed and tailored to best suit the strategic objective of the Group and aligned with the following globally recognized guidelines and standards:

- ISO 31000:2018 – Risk Management Guidelines (“ISO 31000”);
- COSO 2017 Enterprise Risk Management – Integrated Framework (“COSO 2017”); and
- Bursa’s Guidelines: Statement on Risk Management and Internal Control (“SORMIC”).

1.1 Scope

The ERM Framework sets out an overarching overview of strategic risk management building block, guide to perform the risk management process and the methodology that the Group Governance, Risk and Compliance (“GRC”) team is adopting within the Group.



Title : Enterprise Risk Management (ERM) Policy Statement & Framework
Revision : 08
Document No : YHB-RC-CG-PP-0004
Date : 1-Mac-2024

2.0 Ownership

Approver: Board

- This document shall not be altered without the Approver signature.

Checker: Risk Management Function

The Risk Management Function, reporting to the Head of GRC, shall be the maintenance owner of the ERM Policy Statement & Framework ensuring compliance with laws and regulations, formats, coding conventions, content, review cycles, records, sign-off and revision coding.

This procedure is a live document and will undergo periodic review and assessment of its effectiveness and where necessary alignment will be performed.



3.0 Abbreviations and Definitions

The definitions below are the Group standard for all managed documents.

Abbreviations	Descriptions
AC	Audit Committee
BRSC	Board Risk & Sustainability Committee
ERM	Enterprise Risk Management
FPSO	Floating, Production, Storage and Offloading
GRC	Group Governance, Risk & Compliance
MSC	Management & Sustainability Committee
Yinson or “the Group”	Yinson Holdings Berhad



4.0 Enterprise Risk Management Framework Architecture

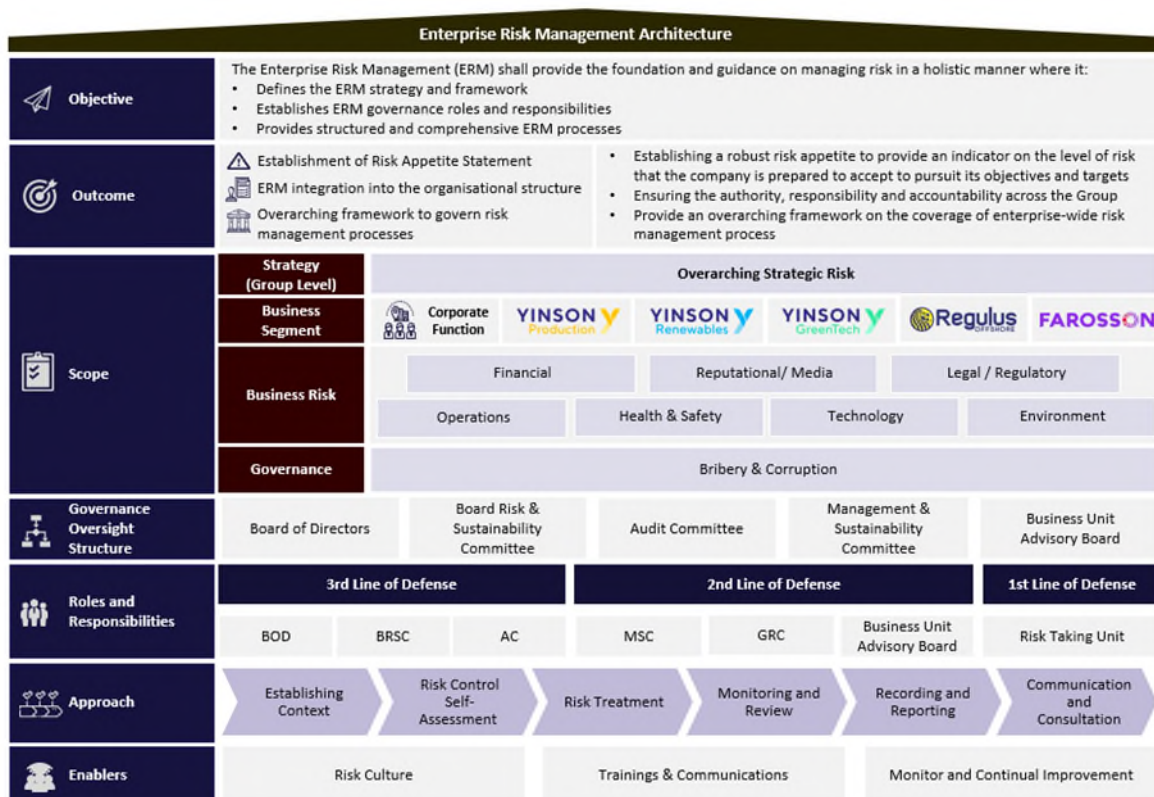
The ERM Framework is designed to strengthen the Group's risk management system and provide an end-to-end coverage of the enterprise-wide risk management governance process. To achieve this, Yinson adopts the Three Lines of Defense model as a foundation for our risk management structure, aligning it closely with the principles and guidelines of ISO 31000.

First Line of Defense – Risk Taking Unit: Our first line of defense lies with our business units and/or departments, who are directly involve in taking risks as part of the operational activities. These units are responsible for identifying, assessing, and managing risks, integrating the Group's risk management practices into daily operations. They maintain a proactive approach to risk, aligning decisions with risk appetites and ensuring compliance with established policies and procedures.

Second Line of Defense – GRC and supporting functions: These functions are responsible for developing and disseminating risk management policies, providing the necessary tools and expertise, driving the right risk culture and overseeing risk management practices across the Group.

Third Line of Defense – Internal Audit: The third line of defense at is an independent internal audit function. This line ensures that both the first and second lines of defense are operating effectively and in accordance with our risk management policies and procedures, as well as the guidelines set out by ISO 31000.

The diagram below, provides an overview of the ERM architecture and sets a foundation content of the ERM Framework.





5.0 ERM Policy Statement & Framework Executive Summary

5.1 Enterprise Risk Management Policy Statement of Yinson Group

Aligned with our commitment to effective risk management, the following policy statements adopted by the Board outline our principles, objectives, and responsibilities regarding risk management.

- **Proactive Risk Management and Risk Culture:** To be fully committed to implementing and maintaining an effective ERM Framework that proactively and adequately identifies, assesses, mitigates, and monitors risks to achieve strategic objectives. Yinson is committed to embed risk considerations into the culture, collective beliefs, values, and behaviors, fostering risk-awareness and resilience throughout the Group by integrating risk management principles and practices into business activities, and decision-making processes.
- **Calculated Approach and Adhering to Predefined Risk Appetite:** The framework advocates the importance of identifying all potential risks, including 'black swan' events, through diligent analysis and leveraging our experiences and industry knowledge. Yinson shall pursue a balanced strategy that focuses on both risk mitigation and value of calculated risk-taking when the potential rewards justify the risks. By applying appropriate governance and controls while considering conservative as well as optimistic outcomes, our framework ensures informed decision-making, enabling us to confidently navigate the risk landscape and achieve sustainable achievements while managing risks within our appetite.
- **Dynamic Adaptation and Continuous Improvement:** Yinson pledges to continuously adapt our risk management practices to the evolving business landscape, leveraging the latest insights and technology to enhance our risk response strategies. This dynamic approach ensures not only compliance with current standards but also a perpetual state of improvement, aligning to best practices and industry standards.



5.2 Risk Appetite and Tolerance

Risk appetite measures the amount and type of risk that the Group is willing to accept in the pursuit of its strategic and operational objectives. Business units are expected to operate within the defined risk appetite thresholds and adopt stringent measures where appropriate. Certain risks that surpass the risk appetite thresholds may still be considered viable, provided there is:

- full awareness and informed consent from relevant management levels;
- implementation of robust and ongoing monitoring measures to closely track the progress and potential impact of the risk; and
- regular reporting to the relevant Board, providing comprehensive updates on the risk's status, any mitigation efforts undertaken, and lessons learned.

Risk Appetite Statement

This section articulates Yinson's risk appetite, defining the level and type of risk that Yinson and its businesses are willing to accept in pursuit of its strategic objectives and business goals.

No.	Key Areas	Risk Appetite
1.	Strategic	Yinson is committed to pursuing innovative growth opportunities and strategic ventures, accepting a low to medium level of residual risk, provided these align with our long-term goals and do not jeopardize our core business stability and integrity.
2.	Financial	Yinson adopts a prudent financial risk management, balancing risk and reward for sustainable growth and stakeholder value. We focus on maintaining financial stability and managing credit, liquidity, and market risks within low to medium levels.
3.	Environment and Sustainability	Yinson is committed to minimise its environmental footprint and promoting sustainable practices. We have a zero tolerance for risks that lead to significant environmental harm or non-compliance with sustainability regulations.
4.	Compliance and Regulatory	Yinson is committed to upholding the highest standards of compliance and regulatory adherence. We have zero tolerance towards any legal, financial, or reputational damage and strive to ensure continuous alignment with evolving regulatory landscapes, maintaining transparency in our operations, and fostering a culture of ethical conduct and compliance throughout the organisation.
5.	Operations	Yinson is committed to operational excellence and maintains a balanced approach aiming for low to medium risk tolerance on our standard operations. We strive to continuously improve our processes, systems, and controls with the goal of minimising disruptions and ensuring robust project execution and business continuity.
6.	Health & Safety	Yinson is committed to maintaining the highest standards of health and safety in all aspects of our operations. We have a zero tolerance policy towards compromising on safety protocols and employee well-being. Yinson strives to keep all health and safety risks as low as reasonably practicable and ensures strict adherence to industry standards and regulatory requirements.
7.	Reputation	Yinson is committed to maintaining and enhancing our reputation as a trustworthy, ethical, and reliable entity across all our business practices and stakeholder interactions with a low tolerance for risks that could lead to a loss of trust or damage to our reputation.
8.	Technology and Cybersecurity	Yinson is committed to maintain a robust and secure technological environment. Yinson encourages adoption of innovative technologies along with stringent controls to drive business growth, tolerating low to medium risk but not at the expense of compromising critical systems' integrity or data security.



6.0 Risk Management Scope

6.1 Strategic Risk Management

The Group adopts the methodology in assessing and formulating the strategic risk point of view moving forward by incorporating strategic risk indicators for decision-making process.

6.2 Corporate Risk Profile based on Business Functions

Corporate risk management focuses on providing the Board and management with a strategic and holistic view of the key risks that is affecting or may potentially affect the Group objectives, as well as supporting the strategic decision-making.

There are eight (8) categories of corporate risks in Yinson as summarised below:

Categories	Definitions
Strategy	Risk that adversely affects the stability and/or integrity of the company as well as its ability to achieve strategic goals and objectives.
Financial	Risks associated with adverse impacts on the company's financial performance and stability including incurring additional/increased liabilities.
Technology and Cybersecurity	Risks arising from the use of technology including cybersecurity breaches, system failures, data loss/breaches, and technological obsolescence, which can disrupt operations and impact business objectives.
Environment and Sustainability	Risks associated with negative environmental impact including failure to adapt and respond to sustainable practices and regulations, which may affect the company's long-term viability. <i>(Refer to Appendix 14.1 on the details of climate-related requirements and risks associated with climate change)</i>
Health & Safety	Risks associated with the potential harm or danger to the physical well-being and safety of individuals due to hazards, conditions, or activities, both on-site and in any company-related activities.
Compliance and Regulatory	Risks arising from non-adherence to laws, relevant regulatory requirements, contractual obligations, and industry standards. (e.g. environmental regulations, labor laws, data protection laws, specific industry compliance requirements, etc.)
Operations	Risks associated with inadequacy or failure of internal processes, people, and systems, or from external events, causing losses, delays or disruptions to project completion or operations of the business and/or key assets.
Reputation	Risks associated with adverse impact to the Group's image, public perception and creditability among its stakeholders, including clients, investors, regulatory bodies, and the general public.



6.3 Strategic Investment, Key Business Activities, and New Projects/Segment

New ventures and projects carry higher risks due to uncertainties in market fit, technology viability, and operational execution. A tailored risk management approach is crucial. This section presents a streamlined strategy, emphasizing the involvement of project sponsors, the risk management team, and key stakeholders in mitigating potential risks to Yinson from new ventures.

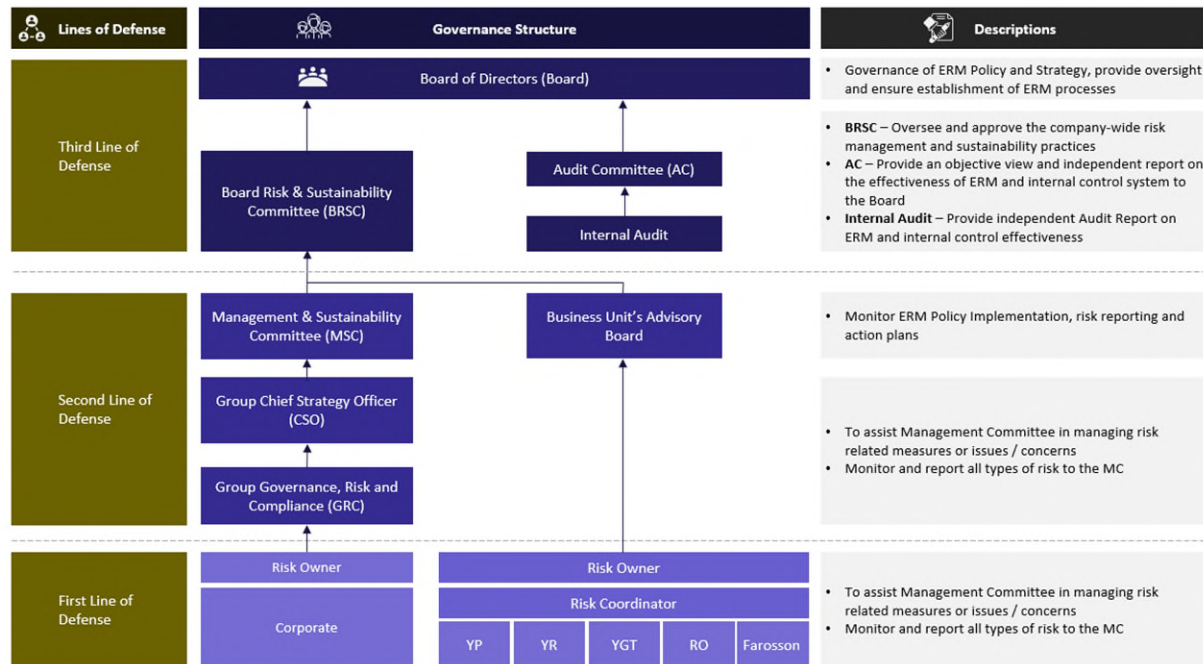
- **Strategic Alignment:** Assessing the alignment of the venture with Yinson's overall strategic goals and objectives and potential risks affecting its visions and resilience.
- **Risk Identification:** Outline the process for pinpointing risks specific to new ventures and projects, focusing on market, technology, and operational uncertainties.
- **Risk Assessment:** Detail the methodology for evaluating the impact and likelihood of identified risks, employing quantitative and qualitative approaches. Highlight the involvement of project sponsors and relevant stakeholders in risk assessment.
- **Mitigation Strategies:** Provide guidelines for developing tailored risk mitigation plans, aligning with the unique challenges of new ventures.
- **Monitoring and Reporting:** Specify mechanisms for continuous monitoring of risks and regular reporting to ensure transparency and timely decision-making.
- **Roles and Responsibilities:** Define clear roles for project sponsors, the risk management team, and stakeholders in the risk management process.
- **Governance and Compliance:** Outline governance structures and compliance requirements, ensuring accountability and adherence to regulatory standards.
- **Review and Adaptation:** Establish procedures for reviewing risk management outcomes and integrating lessons learned into future strategies.

All papers related to strategy, key project approval, significant action, or investment shall be guided by the established Limit of Authority for respective business units.



7.0 Governance Oversight Structure

The ERM Framework governance structure defines the roles and responsibilities of the stakeholders in governing, managing, monitoring, and communicating the risks. The Board is responsible for the supervision and monitoring the principal and strategic risks while the Board Risk & Sustainability Committee (“BRSC”) is responsible for the overall implementation of risk management across Yinson. The governance structure for the Group is shown in the diagram below:





8.0 Roles and Responsibilities

To ensure there is adequate governance in place to govern the risk management system across the Group, the ERM Framework has set forth the detailed roles and responsibilities as follows:

Roles	Principal Responsibilities for ERM
Board of Directors ("Board")	<ul style="list-style-type: none">• Determine the risk appetite for the Group to set the direction for the risk management activities.• Understand the principal enterprise risks relevant to the business of the Group including climate-related risks and recognise the business decisions require risk-taking.• Provide oversight and ensure the establishment of systems that effectively identify, assess, monitor, and manage associated risks with a view to the long-term viability of the Group.• Approve, adopt, and provide oversight on the implementation of ERM Policy Statement & Framework across the Group.• Review and provide feedback on the ERM reports submitted by the BRSC pertaining to the ERM activities of Yinson.
Board Risk & Sustainability Committee ("BRSC")	<ul style="list-style-type: none">• Define overarching risk management strategies including risk appetite and risk management performance measures that aligned to strategic business objectives.• Review, endorse and oversee the implementation of ERM Policy Statement & Framework as well as the effectiveness of risk management processes across the Group.• Review and oversee the management of risks across the Group including climate-related risks with regard to the complexity and significances of these risk exposures.• Review, provide feedback and aggregate the ERM reports submitted by the MSC and Advisory Board of business units to the Board.• Communicate the Board's vision and strategies for risk management to all personnel across the Group.• Promote a healthy risk-aware culture and address factors that could derail the effectiveness of risk management practices across the Group.
Audit Committee ("AC")	<ul style="list-style-type: none">• Review the adequacy and effectiveness of the ERM and Group's internal control system.• Provide an independent view and recommends to the Board on the steps to improve the system of internal control derived from the findings of internal and external auditors.
Internal Audit	<ul style="list-style-type: none">• Assist AC in reviewing the effectiveness of ERM and internal controls while providing an independent view on specific risks and control issues, the state of internal controls, trends, and events.
Management & Sustainability Committee ("MSC")	<ul style="list-style-type: none">• Review the design, implement and monitor the ERM Policy Statement & Framework in accordance with Yinson's strategic vision and overall risk appetite.• Oversee the formal development of ERM policies encompassing all business activities and ensure the development of policy manuals, processes, procedures and practices as well as the business units' adherence to the ERM policies.• Monitor and review the enterprise risks relevant to the business of the Group and the achievement of the Group's objectives and strategies.• Review and assess the adequacy of risk management mitigation plans and internal controls to manage the key enterprise risks for the Group.• Review, provide feedback and aggregate the ERM reports submitted by GRC to the BRSC.



Roles	Principal Responsibilities for ERM
Role	Principal responsibilities for ERM
Group Governance, Risk Management & Compliance (“GRC”)	<ul style="list-style-type: none"> Continuously communicate, evaluate, and improve the ERM Policy Statement and Framework. Facilitate the risk assessment including discussing on emerging risk issues with respective business/ operations areas, implementation, and monitoring of risk action plans. Provide independent input on risk assessment and action plans comprehensiveness. Periodic meetings with senior management of corporate functions and business units to coordinate the risk activities. Prepare and report to the MSC in a timely manner and ensure flash reports are prepared in the event of any new risk(s) that require urgent attention. Ensure climate-related risks and opportunities are being communicated to the MSC and embedded in the ERM process. Lead the ERM educational programs, and continuous sharing insights into risk and market trends with risk owners.
Business Unit’s Advisory Board	<ul style="list-style-type: none"> Ensure the risk management strategies and practices of the respective business unit are in accordance with Group’s ERM Policy Statement & Framework. Review and manage the overall risk profile of the business unit to be consistent with Group’s risk profile, considering the nature, scale and complexity of the operations and using the ERM tools. Report the risk profile and promptly escalate key/ emerging risk issues arising to the Board Committees and Yinson Board, as required and in line with Group’s ERM Policy Statement & Framework. Evaluate and assess the adequacy of controls for managing the overall operational risks associated with business activities. Promote a culture of risk awareness and accountability throughout the business, ensuring that risk management principles are applied in strategy planning and decision making.
Risk Coordinators	<ul style="list-style-type: none"> Drive risk management processes within the business units in identifying, assessing, evaluating, communicating, and monitoring the risks. The Risk Coordinators key roles (but not limited to) include: <ul style="list-style-type: none"> Provide risk awareness/ refresher course/ updates on ERM requirements for respective Management/ Risk Owners; Conduct risk assessment on a quarterly/ need basis; Challenge the risks on a quarterly basis (e.g., monitor during the quarter should any issues arises) and ensure that the risks registered within the risk profiles are kept up-to-date; Monitor all the risk involved and ensure follow-up on action plans introduced before the deadline committed; and Collate the risk profile and report to the Chief Executive Officer (“CEO”) at business unit level before escalation to GRC for further consolidations and review on the risk profile.
Risk Owners	<ul style="list-style-type: none"> Drive effectiveness and ensure accountability as well as accuracy in managing the assigned risks. Perform regular review to identify and assess the risks. Monitor external and internal events that could lead to changes of the risk.



Title : Enterprise Risk Management (ERM) Policy Statement & Framework

Revision : 08

Document No : YHB-RC-CG-PP-0004

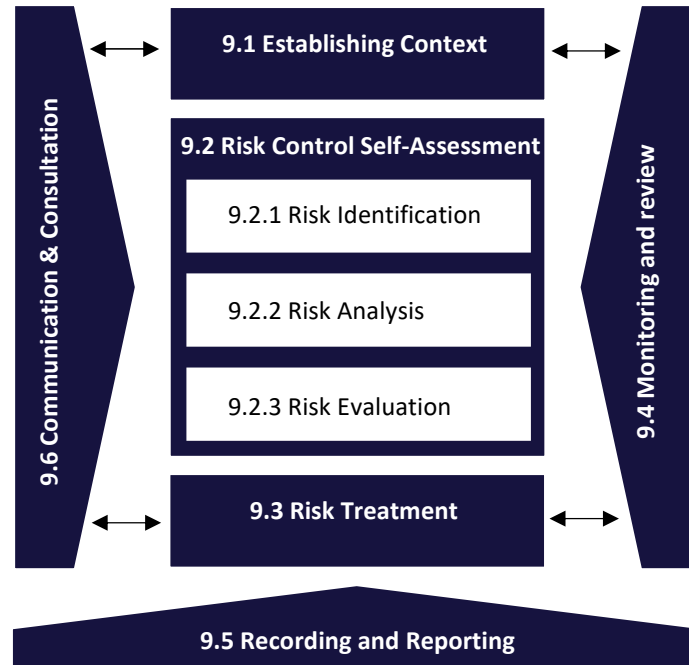
Date : 1-Mac-2024

Roles	Principal Responsibilities for ERM
	<ul style="list-style-type: none">• Proactively identify, drive and oversee implementation of risk action plans to further reduce the likelihood and impact of the risk.• Provide justification and validation of material changes to the risk including the retirement of the risk.• Ensure timely escalation of material events related to the risk to management and GRC.
Risk Co-Owners	<ul style="list-style-type: none">• Provide support to risk owners on key risks identified and to assist in the implementation of risk action plans.• Engage and discuss with risk owners on internal and external activities or circumstances that may give rise to new risks or changes on rating or control effectiveness of existing risks.
Employee	<ul style="list-style-type: none">• Assist risk owners and/ or risk co-owners on key risks identified and to support the implementation of risk action plans.• Engage and discuss with risk owners and/ or risk co-owners on internal and external activities or circumstances that may give rise to new risks or changes on rating or control effectiveness of existing risks.• Exercise care to prevent loss, whilst capitalising the opportunity as well as ensuring the operations, reputation and assets are not adversely affected.



9.0 Enterprise Risk Management (ERM) Process

Yinson adopts the ERM framework outlined by the ISO31000:2018 to facilitate effective identification, assessment, evaluation, treatment, monitoring and reporting of corporate and business associated risks. The overview and interrelation of the ERM framework components is depicted as below:



9.1 Establishing Context

The establishment of context defines the scope and sets the criteria for the development of comprehensive risk management process which in tandem with business needs and requirements as well as enabling effective risk assessment and appropriate risk treatment across the Group. This process entails an assessment and understanding on the business processes and the associated internal and external factors which present potential exposure to the achievement of strategic objectives.

- **Internal Factor**
This refers to factors which influence the way of businesses and resources are managed in achieving the Group's mission, vision, values, and strategic objectives. The scope of internal factor includes (but not limited to) internal stakeholders, governance, process, and system.
- **External Factor**
This refers to the macro-environmental factors which influence the business strategy and direction forward of the Group. The scope of external factor includes (but not limited to) relevant social, economic, technological, environmental, regulatory, legal and, geopolitical factors.



9.2 Risk Control Self-Assessment ("RCSA")

RCSA is a critical component within the framework, designed to identify, assess, manage, and mitigate risks across all levels of the organisation which empowers business units and functions to actively participate in the risk management process by identifying and assessing the risks they face in their day-to-day operations, as well as evaluating the effectiveness of controls in place to mitigate those risks. Yinson shall conduct the risk assessment systematically, interactively, and collaboratively, deriving from the knowledge and views of stakeholders by utilising the best available information which supplemented by further inquiry as necessary.

9.2.1 Risk Identification

This step is the initial and most critical stage which involves recognising risks that could negatively and positively impact the achievement of an organisation, unit or department objectives, noting potential cause and scenario. This process must be conducted during the planning stages of a new initiative, project, structural change, and strategic shift as well as periodically to recognise changes in both internal and external environment.



Risk management is the science of identifying, assessing, and mitigating potential threats to goals and objectives. Therefore, it is important to note that risk represents potential future problems, as opposed to an issue, which is an event that has already occurred. The goal of risk management is to develop preventive controls to reduce the likelihood of the risk materialising, detective controls to monitor materialization of the risk, and ensure the readiness of corrective measures should the risk materialise. Distinctively, issue management focuses only damage control and recovery.

Key areas when creating a risk statement:

- **Clarity and Conciseness:** Briefly describe the risk in simple, understandable language across all relevant stakeholders. Clarity, accuracy, and consistency of this process are crucial for effective assessment, communication as well as driving accountability of controls. Avoid jargon and technical terms that might hinder comprehension.
- **Specificity:** Use specific terms that identify the source, context, and potential impact of the risk. Instead of stating "Project may fail," specify "Potential delay in receiving critical materials could lead to missed project deadline."



Key areas when describing a risk:

- **Context:** Provide background information to explain the source of risk and relevance. Explain why the risk is important and how it relates to your goals. Consider including what would drives the likelihood (i.e. trigger events) and material impact affecting the goals. Possibly, include current status, dependencies, and historical data to further emphasise on the importance of managing the risk.
- **Actionable:** Formulate the description in a way that prompts action. Instead of "Data breach possible," say "Inadequate data security measures could result in a data breach, impacting customer privacy and incurring financial penalties."

9.2.2 Risk Analysis

Risk analysis is the process of diving into the risk, understanding its nature, identifying possible root causes and consequences of the identified risk.

- Identify Possible Root Causes and Consequences

Identify the possible weaknesses, vulnerabilities, or external threats that could trigger create the potential for the risk to occur. Common root causes are human related lapses, ineffective processes, systems, or tools. Otherwise, external events (e.g. technological advancement, changes in regulation, etc.) are other possible root causes. Effective root cause identification leads to effective development of mitigation strategies by addressing root cause, not just the symptoms. Identify Possible Consequences

Identify direct and indirect consequences when the risk materialises by determining financial or non-financial impacts.

Refer to [Appendix 14.3](#) for details on the Risk Impact Rating for Financial Parameter and [Appendix 14.4](#) for Risk Impact Rating for Non-Financial Parameter.

- Determine the Likelihood

Likelihood is defined as the frequency of an event occurring in a stipulated time. Inherent or gross likelihood is the frequency of the risk materialising without taking into consideration of any controls while residual likelihood considers all controls based on its determined effective levels. Following are the relevant techniques that can be utilised in determining the risk likelihood:

- **Quantitative Techniques:** When data is available, use mathematical models to calculate the probability of a risk. This can involve:
 - Historical data analysis: Examining past incidents and near misses to estimate future occurrence rates.
 - Statistical analysis: Utilising industry data or risk databases to assess likelihood based on similar contexts.
 - Fault tree analysis: Mapping out the logical sequence of events that could lead to the risk, calculating the probability of each step.
- **Qualitative Techniques:** These rely on expert judgment and experience to estimate the likelihood of a risk occurring. Methods include:
 - Delphi technique: Anonymously surveying experts to gather diverse perspectives on likelihood.
 - Scenario planning: Envisioning different future scenarios to assess the risk's potential manifestation in each.

Refer to [Appendix 14.2](#) for details on the Risk Likelihood.



- Determine the Impact

Each of the consequences identified to be evaluated based on its financial or non-financial impact parameters. Inherent or gross impact is the unmitigated, potential consequences of a risk without considering any control measures while residual impact considers all controls based on its determined effective levels. While controls rarely address impact, there are some controls that could be reduce the residual impact such as insurance programs, data backups, alternative or redundant systems, etc.

Refer to [Appendix 14.3](#) and [Appendix 14.4](#) for details on the Risk Impact Parameters.

- Determine Gross (Inherent) Risk Rating

Gross or inherent risk rating refers to the intrinsic or unmitigated level of risk in the absence of controls and action plans taken to alter the likelihood and impact.

Refer to [Appendix 14.5](#) for details on the Risk Matrix

9.2.3 Risk Evaluation

Risk evaluation process involve the identification of key controls and evaluation of its effectiveness in reducing the risks to an acceptable level within the organisation's risk appetite.

- Determine Existing Key Controls

Existing key controls that manage the risks are identified and matched to the control types, and control natures outlined below. Controls identified could address one or more root causes and vice-versa.

Control Type	Definitions	Example
Preventive	Measures to prevent risks from occurring.	<ul style="list-style-type: none">• Cybersecurity Awareness Training• ESG Supply Chain Screening
Detective	Measures to identify risks after they have occurred.	<ul style="list-style-type: none">• Compliance audits• Key Risk Indicators (KRI)
Corrective	Measures to correct or reduce risks after they have been detected.	<ul style="list-style-type: none">• Insurance Programs• Data restoration and procedures from backups

Control Nature	Definitions	Example
Manual	Controls performed entirely by human intervention.	<ul style="list-style-type: none">• Physical security inspections such as night petrol and security guards• Training and awareness programs
Semi-automated	Controls performed by a combination of human intervention and automated functionality.	<ul style="list-style-type: none">• Vendor screening through Vendor Registration Platform (VRP) system• Physical access controls such as card key and biometric access systems
Automated	Controls performed entirely by automated functionality.	<ul style="list-style-type: none">• Anti-virus software• Automated data entry



- Determine Control Effectiveness

For risk evaluation, control effectiveness should be assessed and categorized into the following categories:

Control Effectiveness	Descriptions	Example
Effective	<ul style="list-style-type: none">• Addresses the unique nature and vulnerabilities of the specific risk• Well designed and consistently functioning• Meets compliance requirements• Not manually triggered	Installation of firewall, regular tested and maintained fire detection and alarm systems, clearly define acceptable use of technology, data handling practices, and password management guidelines.
Moderately Effective	<p>Positive impact on risk mitigation but :</p> <ul style="list-style-type: none">• Has procedural gaps or lack of adherence• Only addresses some aspect or part of the risk• Effectiveness has decline through time• Requires a material amount of manual intervention to be triggered	Password complexity requirements without multi-factor authentication, transaction monitoring focused on large discrepancies, redundant systems without automatic failover
Ineffective	<ul style="list-style-type: none">• Little to no meaningful impact on risk mitigation• Untested, poorly designed or implemented• Outdated or proven ineffective when events related to risk unfold• Requires significant amount of resources to be triggered• Effective on the risk but triggers the likelihood of inter-related material risks	No data backups or outdated backups, overreliance on single suppliers or resources, physical security cameras with no monitoring and alerts

- Determine Residual Risk Rating

Residual risks are quantified considering the effectiveness of existing controls, and the degree of the impact and likelihood in reducing the gross rating of the risk identified. Significant reduction of gross risk rating should be done in alignment with rating of the existing control effectiveness and justification for the movement shall be reported to GRC.

Refer to [Appendix 11.6](#) for details on the Risk Matrix.

- Risk Profiling

Existing risk profile is prioritised based on the residual risk rating of Critical, High, Medium, or Low



9.3 Risk Treatment

Depending on the residual risk levels and the risk appetite set by the organization, risk treatment process involves identifying the range of options for treating risks, assessing these options, and prioritising the implementation of treatment plans. The risk treatment methodology that the Group is currently practicing is as follows:

Risk Treatment	Descriptions
<u>A</u> voiding	Not starting, discontinuing, terminating an activity that gives rise to the risk. Inappropriate risk avoidance may increase the significance of other risks or may lead to the loss of opportunities for gain.
<u>A</u> ccepting	Retain or accept the risk. Decision of risk retention must be supported with adequate cost-benefit analysis (financial and non-financial).
<u>M</u> odifying	Treatment to modify, such as reducing the magnitude of the likelihood (pre-event) or impact (post-event), or both likelihood and impact of the risk.
<u>S</u> haring	Share the risk with a third party via sub-contracting, joint venture, partnership, and outsourcing or insurance. This usually involves a cost or risk premium such as insurance premium.

Risks that are residually beyond the risk appetite defined are required to be justified that options to avoid or share the risks are unavailable, or the benefits of accepting the current residual risk levels outweigh the potential consequences. The risks must be continuously modified (i.e. development of additional action plans), monitored and reported to the relevant management and Board that all potential root causes and controls had already been addressed and considered in totality.

9.4 Risk Monitoring and Review

Risks across the Group are required to be reviewed, monitored, and re-evaluated by the risk owners on a quarterly basis with facilitation from GRC and risk coordinators for respective business units. The medium of risk review shall be conducted through discussion with risk owners or issuance of questionnaire based on the criticality of the function/ business units. Changes made to the risk register through the risk review shall be updated and reported in the ERM system (i.e. ServiceNow) as the main repository solution for risk data.

To ensure effective monitoring of the risk, Key Risk Indicators (KRIs) should be developed to monitor and review Critical and High residually rated risks that have material impact to the Group (*refer Section 11.0 for the detailed KRI process*). The table below defines the suggested monitoring exercise for respective residual risk rating:

Residual Risk Rating	Criteria
Critical	<ul style="list-style-type: none">Risk that is highly likely or imminent to occur and has severe financial, operational, legal, or reputational damage which may threaten the viability or integrity of the company;Highest priority of the relevant management and requires immediate and extensive action which may include potential mobilisation of the entire organisation, to mitigate or manage the risk;Risk must be reported and thoroughly deliberated to BRSC; and(Early warning where possible) KRI development is required for immediate response planning and crisis management.
High	<ul style="list-style-type: none">Risk that is likely (potentially frequently) to occur and has serious consequences that could disrupt operations or damage the company's reputation and/or finances but may not be severe enough to threaten the viability or integrity of the organization;Proactive and comprehensive management required where considerable number of resources or implement strategic changes to mitigate the risk;



	<ul style="list-style-type: none">• Risk must be reported to BRSC while deliberation is subject to the request of senior management, or Board members; and• KRI development is required to allow close monitoring, timely & effective actions to be taken as well as better resource allocation.
Medium	<ul style="list-style-type: none">• Risk that may occur occasionally and has moderate consequences that may lead to some disruption to operations, reputation and financial that are manageable through standard risk management processes; and• Requires regular monitoring and specific policies or procedures to manage effectively.
Low	<ul style="list-style-type: none">• Risk that rarely or infrequently occurs and has minimal or negligible consequences and easily manageable without much impact to operations, reputation and finances; and• Routine management are sufficient to address these risks with no significant resource allocation required.

9.5 Risk Retirement

Risk retirement is a process where an existing risk is being removed from the risk register with adequate justification and validation from the risk owner. To ensure that risks are being retired in systematic and controlled manners, the risk retirement process shall be guided by the following steps:

i. Justification and Validation from Risk Owner

The risk owner is required to provide adequate justification and validation for the risk retirement with a proper documentation in the risk register via ERM system. There are several possible criteria for a risk to be retired, which as follows:

- The risk is no longer relevant to the function/ business unit (e.g. COVID-19)
- The risk has been minimized beyond acceptable level. It will continue to be monitored operationally by the function/ business unit as part of business-as-usual (“BAU”) process.
- The risk has now become a subset or being monitored via another risk.
- The risk has been transferred to an external party. Transitional risk arising from risk transfer must be adequately monitored by the function/ business unit operationally

ii. Concurrence on Decision by GRC

Subsequent to the justification and validation from risk owners on the risk retirement, the decision must be concurred through discussion with GRC to ensure the retirement of the risk is aligned with ERM policy and practices.

iii. Approval by Department Head or Business Owner

With the mutual agreement between the risk owner and GRC on the risk retirement, final approval from the department head or business owner is required to ensure that the decision to retire the risk is endorsed at a higher level of authority across the Group.



9.6 Risk Reporting

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

Reporting Party	Reporting to	Reporting Frequency	Report to be Submitted
Management & Sustainability Committee (“MSC”)	<ul style="list-style-type: none">Board Risk & Sustainability Committee (“BRSC”)Board	Quarterly	<ul style="list-style-type: none">Risk action plans and Key Risk Indicators updates for Top 5 risksCorporate Risk ProfileBusiness Segment Risk ProfileClimate Risk ProfileSpecial risk report on need basis
Business Unit’s Advisory Board	<ul style="list-style-type: none">Board Risk & Sustainability Committee (“BRSC”)Board	Quarterly	<ul style="list-style-type: none">Business Segment Risk ProfileStatus progress update on the key risk action plansSpecial risk report on need basis
Group Governance, Risk & Compliance Department (“GRC”)	<ul style="list-style-type: none">Management & Sustainability Committee (“MSC”)	Quarterly	<ul style="list-style-type: none">Risk action plans and Key Risk Indicators updates for Top 5 risksCorporate Risk ProfileClimate Risk ProfileBusiness Segment Risk ProfileStatus progress update on the key risk action plansSpecial risk report on need basis
Risk Coordinator	<ul style="list-style-type: none">Business Unit’s Advisory Board	Quarterly	<ul style="list-style-type: none">Updated individual risk register and risk profiles for key risks of business unitRisk action plans and KRI updatesSpecial risk report on need basis
Risk Owners / Risk Co-Owners	<ul style="list-style-type: none">Group Governance, Risk & Compliance Department (GRC)Risk Coordinator	Quarterly	<ul style="list-style-type: none">Updated risk register and risk profiles of each business unit / departmentDetailed risk action plans and status updatesSpecial risk report on need basis
Internal Audit	<ul style="list-style-type: none">Audit Committee (AC)	Annually	<ul style="list-style-type: none">Independent report on the effectiveness of internal controls and risk management implementation



9.6.1 Immediate Risk Escalation

In the event of, or upon the identification of, a significant triggering event or material change to a risk, there might be a need for immediate escalation of the situation to senior management or the Board. This applies to scenarios in the following manner:

- **Material Change of The Risk:** when a change occurs that suggests a material change to the likelihood or impact of a previously identified risk, and where this change indicates the risk may now exceed the established risk appetite
- **Material Triggering Event:** during the occurrence or discovery of an event that has impact of Moderate and above based on the defined risk impact parameters.

In the event of the scenario occurs, the escalation process shall take place as follows:

- The individual or team identifying the risk event or material change must immediately notify their line manager and GRC which assesses the situation and conduct a preliminary evaluation of the potential impact on the organisation or business.
- Based on the assessment and concurrence of the affected function / business units, GRC will:
 - Escalate the issue to senior management or the Board depending on the severity and urgency of the situation.
 - Provide a clear and concise report outlining the risk event or material change, its potential impact, and any recommended mitigation actions.
 - Work collaboratively with relevant departments to develop and implement an appropriate response plan.

9.7 Communication and Consultation

Effective communication ensures that those responsible for implementing risk management and those affected by risks and risk policies understand the rationale behind decisions and the risk management process itself. The purpose of having close coordination between communication and consultation is to drive transparency and facilitate factual, timely, relevant, accurate and understandable exchange of information within and throughout all steps of risk management process.



10.0 Emerging Risk

Emerging risks are new or evolving threats that have not yet fully materialized or become mainstream. They can be difficult to predict and quantify, but potentially hold significant consequences for your organisation. Proactive identification and management of emerging risks offer several benefits:

- **Enhanced preparedness:** Early awareness allows for proactive mitigation and contingency planning, minimising potential impact.
- **Competitive advantage:** Gaining a head start on understanding and addressing emerging risks can lead to innovation and improved resilience.
- **Informed decision-making:** Integrating emerging risks into strategic planning helps make informed choices considering future possibilities.
- **Reputation management:** Anticipating and addressing emerging risks demonstrates proactive risk management and fosters trust with stakeholders.

10.1 Identification of Emerging Risk

There are various identification techniques to identify emerging risks given its distinct characteristics, including, but not limited to:

- **SWOT Analysis:** SWOT Analysis helps identify the emerging risks from a broader perspective based on strengths, weaknesses, opportunities, and threats that could affect strategy or operations. It aims to minimise adverse effects while maximising potential opportunities.
- **Horizon Scanning:** Horizon Scanning helps predict and evaluate early signs of emerging risks across designated timeframes of short, medium, and long term.
- **External Consultation:** Engage with industry experts, analysts, or consultants that are specialised in emerging risk identification related to the business Yinson is exposed to.

Following the identification techniques of emerging risks, the subsequent risk management process as outlined in Section 9.0 remains applicable.



11.0 Key Risk Indicator (“KRI”)

Key Risk Indicator (“KRI”) constitutes a set of measurable parameters used to provide early warning signals indicating potential risk materialisation or an escalating risk exposure. To ensure effective risk monitoring, KRI is required to be developed for Critical and High residually rated risks across the Group.

11.1 KRI Requirements

An effective KRI should possess the following characteristics:

Characteristic	Definition
Relevance	KRI should be directly related and aligned to the risks.
Sensitivity	KRI should be sensitive enough to detect changes or trends in risk factors before they escalate into major issues.
Measurability	KRI should be quantifiable or, in the case of qualitative KRI, clearly defined and observable. The KRI must be based on data that can be consistently collected and monitored over time.
Specificity	KRI should avoid being overly broad or general. It should be specific and focused on a particular aspect of risk to pinpoint the source of the risk, enabling the implementation of precise mitigation measures.
Consistency	KRI should offer consistent and reliable data over time, enabling accurate tracking of changes and trends in risk factors.
Actionable	When a KRI indicates an elevated risk, it should be able to provide clear actionable information to address the risk and prevent adverse outcomes.
Ownership	KRI should have designated owners to be responsible for monitoring the KRI and taking appropriate actions when necessary.
Communication	KRI should be clearly understandable by relevant stakeholders. Key stakeholders should be informed of any significant changes or breaches of threshold values.

KRI should be categorised as either leading indicators or lagging indicators:

	Leading Indicators	Lagging Indicators
Definition	Forward-looking indicators that provide insights into potential future risk.	Indicators that evaluate past performance and assess the impact of completed actions.
Framing	Future Oriented Example: Percentage of Unresolved Critical Issues	Past Oriented Example: Long Time Injury
	Performance Goals Example: Milestone Achievement Rate	Outcome Measures Example: Customer Satisfaction Index
	Predictive Example: Scope Creep Probability Index	Actuarial Example: Cost Variance Deviation Index
	Process Focused Example: Communication Response Time	Organisational Focused Example: Vendor Performance Index



11.2 KRI Process

11.2.1 KRI Identification

KRI identification process involves identifying existing measurable metrics linked to the risk. Start by analysing the metrics, assessing gaps, and interviewing relevant stakeholders. Focus on indicators that track changes in risk profiles or control effectiveness, prioritizing forward-looking and historical data over absolute values. A well-balanced combination of leading and lagging indicators is important to ensure effective risk monitoring as the leading indicator is predictive in nature that provides early signals of potential risk escalation while lagging indicators offer insights into the historical data which will help in identifying the risk trends. The KRI selected by the risk owners are to be validated by GRC to ensure compliance to the requirements outlined in Section 11.1.

11.2.3 Setting Thresholds

Once the suitable indicators have been selected, the risk owners shall determine the trigger levels of the KRI based on the Red, Amber and Green (“RAG”) limits, which defined as below:

KRI Trigger	Definition
Green	Green represents a safe or acceptable zone. When a KRI is within the green limit, it indicates that the associated risk is within the acceptable range and there is no immediate cause for concern.
Amber (1st Trigger)	Amber is a cautionary or moderate-risk zone. When a KRI enters the amber limit, it suggests that the associated risk is approaching a level of concern. It serves as a signal that attention may be required and proactive measures should be considered.
Red (2nd Trigger)	Red indicates a critical or high-risk zone. When a KRI surpasses the red limit, it signifies that the associated risk has exceeded the acceptable threshold and requires immediate attention. Action plans and risk mitigation strategies should be activated promptly.

The thresholds setting should coincide with Yinson’s risk appetite statement and industry tolerance levels to provide a basis for gauging the acceptability of risk exposure. Respond actions shall be developed for Amber and Red trigger levels in ensuring adequate measures are in place to mitigate further escalation of risk exposures.

There are circumstances where metrics are only available for the identification of a binary KRI. The definition of Red and Green “RG” limits should apply where once the metrics surpasses the red limit which acts as the first trigger, action plans and risk mitigation strategies should be activated promptly.

11.2.4 KRI Tracking and Reporting

The status of established KRI shall be reviewed and monitored by the risk owner on quarterly basis or based on the frequency of the data available for the indicators. In the event of KRI surpasses the Amber and Red limits, proper escalation shall be made to the relevant committees (i.e. MSC, Advisory Board, BRSC) on the KRI status and respond actions taken to mitigate the risk.



12.0 Scenario Planning

Scenario planning is a strategic planning tool for proactively identifying and assessing potential future risks and opportunities based on differing future possibilities. Within the context of ERM, scenario planning involves creating detailed, plausible scenarios that reflect a range of potential future states, helping business anticipate changes, identify emerging risks, and seize opportunities as well as allowing a more robust and flexible risk management strategy in maintaining competitive edge and ensuring long-term sustainability.

Scenario planning involves creating plausible future scenarios based on different assumptions about key drivers like:

- **Technological advancements:** Artificial intelligence, autonomous vehicles, etc.
- **Sustainability demand:** Rate of change in weather conditions, public concerns, etc.
- **Economic trends:** Global recession, regional instability, etc.
- **Regulatory changes:** New data privacy laws, carbon pricing, subsidies, environmental regulations, etc.
- **Geopolitical shifts:** Trade wars, riots, international conflicts, etc.
- **Social and cultural changes:** Changing demographics, consumer preferences, etc.

Scenario Planning for Your ERM: A 5-Step Guide

- **Define:** Identify key areas and objectives for scenario planning (e.g., industry shifts, regulatory changes).
- **Select:** Choose diverse scenarios encompassing best, worst, and middling future possibilities.
- **Analyze:** Assess each scenario's impact on your organization (finance, operations, compliance, reputation, stakeholders). Identify key risks and opportunities.
- **Respond:** Develop contingency plans to mitigate risks and capitalize on opportunities in each scenario. Prioritize actions based on likelihood and impact.
- **Communicate & Monitor:** Share findings and plans with stakeholders. Regularly monitor the landscape and update scenarios as needed.



13.0 Enterprise Risk Management (ERM) Enablers

Integrating risk management in an organisation is a dynamic and iterative process which requires collaboration among multiple business units of different sizes, scope, and capability. Hence in ensuring the effective implementation of ERM across the Group, Yinson shall empower and leverage on the identified key enablers to push for the risk agenda and promote robust risk management understanding to the stakeholders.

13.1 Risk Culture

Risk culture reflects the collective norms, values, attitudes and behaviors of the employees towards risk which form a vital factor in ensuring successful implementation of a comprehensive ERM process across the Group. An effective risk culture is the one that enables and rewards individuals and groups for taking the right risks in an informed manner which will result in earlier identification of risk, allowing the opportunity to develop a collaborative response, ultimately leading to a more resilient organisation. In effort to successfully develop and inculcate the desired risk culture, Yinson shall consider the following key aspects:

Key Aspects	Descriptions
Tone from the top	<ul style="list-style-type: none">• Demonstration of clear commitment and direction by the top management that flow throughout the Group• Strong encouragement to uphold ethical values and integrity in business practices
Decision making	<ul style="list-style-type: none">• Taking into account the risk management perspective in strategic and operational decision-making process• Translate risk strategy into operational and tactical objectives
Collaboration	<ul style="list-style-type: none">• GRC provide advisory role to business function in risk related matters• Develop collaborative working relationship between GRC and business function
Ownership and accountability	<ul style="list-style-type: none">• Clarify clear risk management responsibility and accountability of specific risks by the business functions• Establish risk management as an integral part of day-to-day program and operational management
Education and training	<ul style="list-style-type: none">• Inclusion of risk awareness briefing as part of compulsory induction program for new hires• Conduct technical training and awareness session for the associated risk personnel across the Group• Sharing of risk related reading materials and reference sources via YNet platform



13.2 Trainings and Communications

Yinson shall strive to constantly develop the risk management identification and assessment capabilities of the employees through training and educational programs which will be tailored accordingly to the respective audience for effective communication. In championing this agenda, risk awareness briefing shall be included as a compulsory session within the induction program for new hires and periodic risk training programs shall be continuously conducted for all risk personnel across the Group. Besides that, GRC shall develop and share risk related reading materials as well as reference sources via the YNet platform with purpose to educate and promote risk culture within all employees in Yinson.

13.3 Monitor and Continual Improvement

Effective monitoring and reviewing of the risks associated with the Group shall be conducted continuously to ensure the risk registers and action plans remain relevant within the fast-changing business environment and the alteration of risk profiles due to any changing circumstances are properly documented. The monitoring and reviewing of risks across the Group are being deployed and implemented through the following practices:

Process	Description
Continuous Monitoring and Assessment	<ul style="list-style-type: none">• The Head of Department / Business Unit shall appoint a dedicated person-in-charge to conduct regular monitoring of the risks associated with respective function through routine checking against the risk parameters.• Continuous assessment on the existing, changing, emerging and new risks shall be conducted through line management review to ensure adequate action plans are in place to address the associated risks.
Review and Reporting	<ul style="list-style-type: none">• GRC shall conduct risk discussion with respective department / business unit quarterly to review the existing risks, assess the emerging risks as well as the action plan implementation status. GRC is also responsible to review the appropriateness and completeness of risk profiles and produce consolidated risk report for submission to the MC.• The MC shall deliberate the risk report and ensure sufficient action plans have been set in place to address the highlighted key risks.• The BRSC is required to review all reports / risk information escalated by the MC and seek further clarification directly from the GRC, as deemed necessary. In particular, the BRSC shall review and assess the effectiveness and appropriateness of the risk treatment for high-rated risks and monitor the completion of approved action plans against the agreed timeline.• The Board shall review, comment and adopt the risk-related reports submitted by BRSC on the ERM implementation across the Group.
Benchmarking and continual improvement	<ul style="list-style-type: none">• GRC shall periodically benchmark the implementation of ERM process across the Group against the best practices in industry to ensure continual improvements and enhancement on the existing ERM process.












14.0 Appendix

The following section documents and furnishes the detailed process flow, procedures, policies, templates, etc. that will be used or utilised by GRC to govern the ERM Framework and process to identify, assess, evaluation and monitor the risk within the Group.

Appendix 14.1 – Climate Risk Assessment

At Yinson, we believe that climate change should intrinsically be part of risk management processes, as it can lead to both financial and non-financial risks. Nonetheless, the integration of climate-related risks into our existing ERM processes requires that we be cognisant of the unique characteristics of such climate-related risks. In terms of the range of implications of climate change, it is widely recognized that continued emission of greenhouse gases will cause further warming of the Earth and that a warming above 2°C, relative to the preindustrial period, could lead to catastrophic economic and social consequences. These implications include potential impacts on human health, infrastructure, transportation systems, energy, food, and water supply. For Yinson, this means climate change can affect our assets and operations, supply and distribution chains, employees, and clients. Figure 11-1 indicates the likely physical and economic impacts due to rising global temperature in this century.

Figure 11--1 Physical and economic Impacts due to rising global temperature by year 2100.

Warming by 2100		<2°C		3°C	5°C
Physical Impacts		1.5 °C	2 °C		
	Sea-level rise	0.3-0.6 m	0.4-0.8 m	0.4-0.9 m	0.5-1.7 m
	Chance of ice-free Arctic summer	1 in 30	1 in 6	4 in 6 (63%)	6 in 6 (100%)
	Frequency of extreme rainfall	+17%	+36%	+70%	+150%
	Increase in wildfire extent	x1.4	x1.6	x2.0	x2.6
	People facing extreme heatwaves	x22	x27	x80	x300
	Land area hospitable to malaria	+12%	+18%	+29%	+46%
Economic Impacts					
	Global GDP impact (2018: \$80tn)	-10%	-13%	-23%	-45%
	Stranded assets	Transition: fossil fuel assets (supply, power, transport, industry)		Mixed: some fossil fuel assets and some physical stranding	Physical: uninhabitable zones, agriculture, water-intensive industry, lost tourism
	Food supply	Changing diets, yield loss in tropics		24% yield loss	60% yield loss, 60% demand increase



Given the wide-ranging implications of climate change in both the short and longer time horizon, assessing associated risks will involve dealing with a set of complex interconnecting, many of which operate at different temporal and spatial scales. A critical aspect of integrating climate-related risks into our existing ERM processes involves taking into consideration unique characteristics of climate-related risks as follows:

- **Different effects based on geography and activities**

The effects of climate change and climate-related risks occur on local, regional, and global scales with varied implications for our different businesses, assets, markets, operations, and value chains.

- **Longer time horizons and long-lived effects**

Some climate-related risks exist and play out over time horizons that stretch beyond traditional business planning and investment cycles. These risks and related impacts may occur as a result of decade-long changes in driving forces (e.g., greenhouse gas concentrations in the atmosphere) leading to climate-related physical or transition risk changes over the short, medium, and long term.

- **Novel and uncertain nature**

Many of the effects of climate change have no precedence, limiting the ability to apply statistical and trend analysis based on historical data. Further, climate change is a dynamic and uncertain phenomenon, resulting in complex possible mitigation responses with many unknowns. Such mitigative responses may include development and deployment of critical technologies and adaptation strategies to changing market and consumer behaviors.

- **Changing magnitude and nonlinear dynamics**

Climate-related risks may manifest at different scales over time, with increasing severity and scope of impacts. Climate systems may exhibit thresholds and tipping points that result in large, long-term, abrupt, and possibly irreversible changes. Therefore, understanding the sensitivities of tipping points in the physical climate system as well as in ecosystems and society is essential for understanding climate-related risks.

- **Complex relationships and systemic effects**

Risks associated with climate change are interconnected across socioeconomic and financial systems. Such interconnected risks are often characterized by knock-on effects and systemic effects, requiring a multidimensional perspective to assess the short-, medium-, and long-term implications for our businesses.



Principles for Integration of Climate-Related Risk

In view of the unique characteristics of climate-related risks, we adopted key principles based on TCFD's guidance in the integration of climate-related risks into our ERM processes. The principles support the inclusion of climate change considerations into the elements of risk management processes consistently and proportionately, considering other risks to which our risk management process applies. Interconnections between climate-related risks and other risks shall be considered as part of the integration process and where the existing elements will be applied to a limited business or strategic planning horizon, integration shall consider the longer time horizons over which climate-related risks might materialize. The key principles adopted for integration of climate-related in our ERM processes are as follows:

- **Interconnections**

Integrating climate-related risks into existing risk management requires analysis and collaboration across our businesses. The principle of interconnections means all relevant functions, departments, and experts are involved in the integration of climate-related risks into our risk management processes and in the ongoing management of climate-related risks.

- **Temporal Orientation**

Climate-related physical and transition risks shall be analyzed across short-, medium-, and long-term time frames for our operational and strategic planning, which may require extending beyond traditional planning horizons.

- **Proportionality**

The integration of climate-related risks into existing risk management processes should be proportionate in the context of our non-climate-related risks, the materiality of its exposure to climate-related risks, and the implications for our strategy.

- **Consistency**

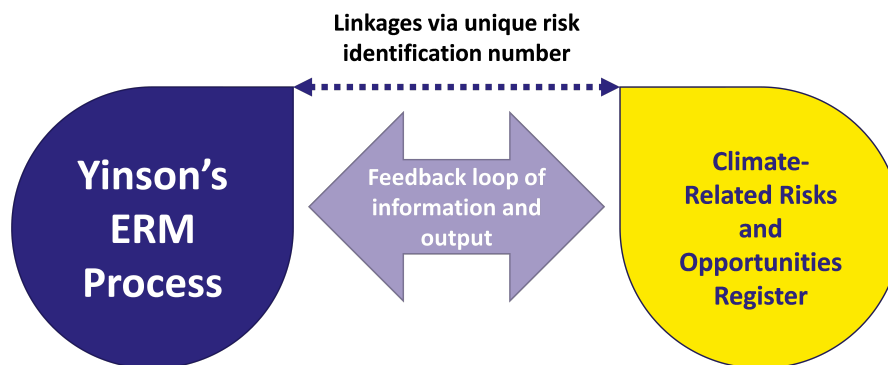
The methodology used to integrate climate-related risks should be used consistently within our ERM processes to support clarity on analysis of developments and drivers of change over time.



Integrating Climate-Related Risks into ERM Process

Each of the risks identified in the risk assessment as part of the ERM processes contains a **unique risk identification number**. The risks identified could be related or not related to climate risks, thus, a thorough consideration shall be given when determining the root causes of the risk identified. If the root causes are linked to climate-related events (either due to transition to low carbon economy or extreme physical weather events), the identified risk shall be earmarked, and linkages shall be established to Yinson's climate-related risks and opportunities register. A simple illustration of the relationship between Yinson's ERM process and the climate-related risks and opportunities register is shown in Figure 11-2.

Figure 11-2 Illustration of the relationship between ERM process and climate-related register



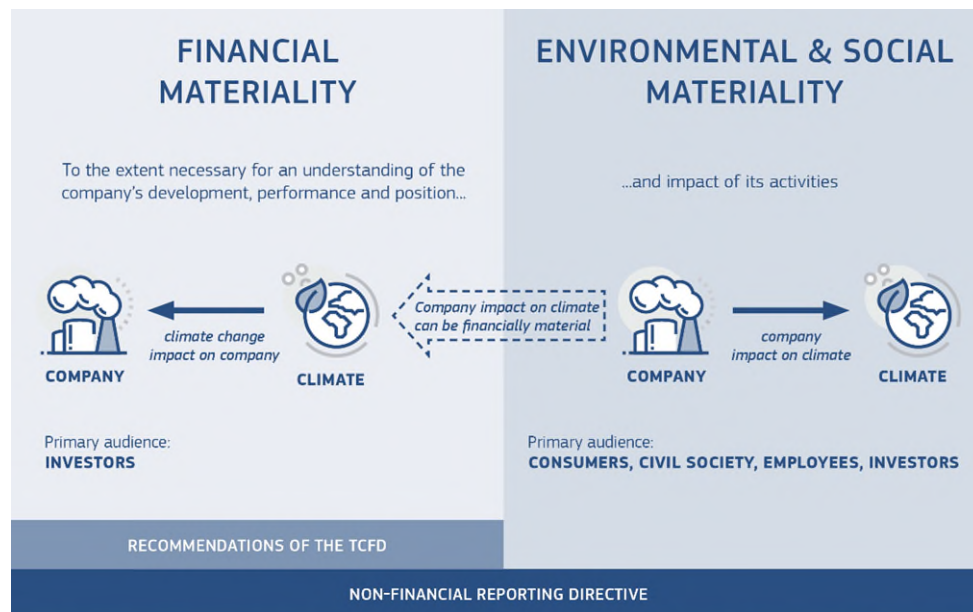
Yinson's Climate-Related Risks and Opportunities Register

The climate-related risks and opportunities register is a dedicated register used specifically to capture the climate-related risks and opportunities of our businesses. This register is a supplement to link the overall Yinson's ERM processes with climate-related risks. This register also serves as a feedback document to the existing risk management process to capture medium- to long-term climate-related risks which could be overlooked in the short-term basis.

It is to note that the climate-related risks shall consider both the impacts/ causes to and from external environments. We adopt the concept of "double materiality" while we consider climate related risks. In other words, while materiality is the effect of climate change on finance and corporate activities, double materiality includes the effect of finance and corporate activities on climate change. Figure 11-3 depicts the concept of double materiality for climate change impact.



Figure 11-3 Double materiality for climate change impact



* Financial materiality is used here in the broad sense of affecting the value of the company, not just in the sense of affecting financial measures recognised in the financial statements.

Defining Climate-Related Risk Drivers

We adopt the climate-related risks categorisation based on TCFD guidance. Broadly, the climate-related risks are divided into two major categories; risks related to the transition to a lower-carbon economy (Transition Risks) and risks related to the physical impacts of climate change (Physical Risks).

Transition Risk

Transitioning to a lower-carbon economy may entail extensive policy, legal, technology, and market changes to address mitigation and adaptation requirements related to climate change. Depending on the nature, speed, and focus of these:

- Policy Risks

Policy risks generally fall into two categories, that is policy actions that attempt to constrain actions that contribute to the adverse effects of climate change or policy actions that seek to promote adaptation to climate change. Some examples include implementing carbon-pricing mechanisms to reduce GHG emissions, shifting energy use toward lower emission sources, adopting energy efficiency solutions, encouraging greater water efficiency measures, and promoting more sustainable land-use practices.

- Legal Risks

Legal risks, or commonly also referred to litigation risks typically arise (in a climate-related context) due to failure of an organization to mitigate impacts of climate change, failure to adapt to climate change, and the insufficiency of disclosure around material financial risks. In recent years, we have seen an increase in climate-related litigation claims being brought before the courts by property owners, municipalities, states, insurers, shareholders, and public interest organizations. As the value of loss and damage arising from climate change grows, litigation risk is also likely to increase.



- Market Risks

While the ways in which markets could be affected by climate change are varied and complex, one of the major ways is through shifts in supply and demand for certain commodities, products, and services as climate-related risks and opportunities are increasingly taken into considerations.

- Technology Risks

Technology risks typically manifest with the development and use of emerging technologies such as renewable energy, battery storage, energy efficiency, and carbon capture and storage. This affects the competitiveness of our businesses through areas such as operational costs, and ultimately demand for our services from end clients. To the extent that new technology displaces old systems and disrupts some parts of the existing economic system, winners and losers will emerge from this “creative destruction” process.

- Reputation Risks

Climate change has been identified as a potential source of reputational risk tied to changing customer or community perceptions of an organization’s contribution to or detracting from the transition to a lower-carbon economy

Physical Risks

Physical risks resulting from climate change can be event-driven (acute) or longer-term shifts (chronic) in climate patterns. Physical risks may have financial implications for our business, such as direct damage to assets and indirect impacts from supply chain disruption.

- Acute Risks

Acute physical risks refer to those that are event-driven, including increased severity of extreme weather events, such as cyclones, hurricanes, or floods.

- Chronic Risks

Chronic physical risks refer to longer-term shifts in climate patterns (e.g., sustained higher temperatures) that may cause sea level rise or chronic heat waves.

Selection of Climate Scenarios for Analysis

A scenario describes a path of development leading to a particular outcome. Scenarios are not intended to represent a full description of the future, but rather to highlight central elements of a possible future and to draw attention to the key factors that will drive future developments. It is important to remember that scenarios are hypothetical constructs; they are not forecasts, predictions, nor are they sensitivity analyses. Scenario analysis is a tool to enhance critical strategic thinking. A key feature of scenarios is that they should challenge conventional wisdom about the future. In a world of uncertainty, scenarios are intended to explore alternatives that may significantly alter the basis for “business-as-usual” assumptions.

The purpose for application of climate scenarios is to consider and better understand how we might perform under different future states (i.e., its resiliency/robustness). In the case of climate change, climate-related scenarios allow us to explore and develop an understanding of how the physical and transition risks and opportunities of climate change might plausibly impact the business over time. Scenario analysis, therefore, evaluates a range of hypothetical outcomes by considering a variety of alternative plausible future states (scenarios) under a given set of assumptions and constraints.



A critical aspect of scenario analysis is the selection of a set of scenarios that cover a reasonable variety of future outcomes, both favourable and unfavourable. While there is an almost infinite number of possible scenarios, we will use a limited number of scenarios to provide the desired variety. In this regard, based on the TCFD guidance, we have selected a 2°C scenario, i.e. Sustainable Development Scenario (SDS) and other scenario such as Stated Policies Scenario (STEPS), and physical climate risk scenario, such as Representative Concentration Pathways (RCP) 8.5.

Stated Policies Scenario (STEPS)

This is based on the stated policies by governments around the world today, which tracks global warming to below 3°C.

Sustainable Development Scenario (SDS)

This scenario is in addition to STEPS, where it is characterized by a larger investment push for clean, renewable energy in the next ten years. This yields far fewer greenhouse gas emissions than the STEPS and it caps global warming at 2°C.

Representative Concentration Pathways (RCP) 8.5

In RCP 8.5, it is assumed that emissions continue to rise throughout the 21st century. Since IPCC AR5, this has been perceived to be very unlikely, but still possible as feedbacks are not well understood. RCP8.5 remains useful for its aptness in both tracking historical total cumulative CO₂ emissions and predicting mid-century (and earlier) emissions based on STEPS. We will utilise the RCP 8.5 scenario for physical risk analysis purposes only.

Time Frame Selection

For the purpose of climate-related risk assessment, it is important to define the time frame for short, medium, and long term as climate-related impacts will be different. For consistency, the risk assessment time frame will be set at year 2025, 2030, 2040 and 2050 for every adopted scenario to manage the relevant short-, medium- and long-term risks. This setting would give a reasonable snapshot at each time frame to understand the transition of climate-related risk.

Organisational Ownership

GRC along with the Corporate Sustainability function will be the custodian for the Climate-related Risks and Opportunities assessment, with the Corporate Sustainability function acting as facilitator. The assessment relies on inputs and collaborations from all businesses and internal organisational functions as the impact of climate-related risk will span across all our operations. The result of the assessment is reported to the BRSC and Board on a quarterly basis.

Revision of Climate-Related Assessment

The climate-related risks and opportunities register shall be updated in a timely manner using appropriate media on an annual basis at minimum within the main annual report.



Climate-Related Documents of References

The climate-related assessment will be based on the following (but not limited to) documents of references:

- TCFD, Final Report: Recommendations of the Task Force on Climate-related Financial Disclosures, June 2017;
- TCFD, Guidance on Risk Management Integration and Disclosure, October 2020;
- TCFD, Guidance on Scenario Analysis for Non-Financial Companies, October 2020;
- TCFD, Technical Supplement: The Use of Scenario Analysis in Disclosure of Climate-Related Risks and Opportunities, June 2017;
- IEA, World Energy Outlook 2020, October 2020;
- IPCC, Fifth Assessment Report (AR5), 2015; and
- IPCC, Climate Change 2021, The Physical Science Basis, August 2021.



Appendix 14.2 – Risk Likelihood Description

Likelihood	Likelihood Description	Frequency
Almost Certain	The risk will occur in most circumstances or at frequent intervals.	More than 50% chance of occurring in the next one year.
Likely	The risk is expected to occur at most circumstances.	10% to 50% chance of occurring in the next one year.
Possible	The risk may occur at some period.	1% to 10% chance of occurring in the next one year.
Unlikely	The risk is likely to occur less frequently.	1% to 10% chance of occurring in the next 10 years.
Rare	The risk may occur in exceptional circumstances.	Less than 1% chance of occurring in the next 10 years.



Appendix 14.3 – Detailed of Risk Impact Rating for Financial Parameters

Factor	Financial Impact (in RM)				
	Insignificant	Minor	Moderate	Major	Catastrophic
Tier 1: Yinson Group					
Profit After Tax (RM 637M)*	Decrease by < than 20% (< RM 127M)	Decrease by 20% - 40% (RM 127M – RM 259M)	Decrease by 40% - 60% (RM 259M – RM 382M)	Decrease by 60% - 80% (RM 382M – RM 509M)	Decrease by > 80% (> RM 509M)
Total Revenue (RM 6,006M)*	Decrease by < than 6% (< RM 360M)	Decrease by 6% - 13% (RM 360M – RM 781M)	Decrease by 13% - 20% (RM 781M – RM 1,201M)	Decrease by 20% -25% (RM 1,201M – 1,502M)	Decrease by > 25% (> RM 1,502M)
Total Cost (RM 4,175M)*	Increase by < than 6% (< RM 251M)	Increase by 6% - 13% (RM 251M – RM 543M)	Increase by 13% - 20% (RM 543M – RM 835M)	Increase by 20% - 25% (RM 835M – RM 1,044M)	Increase by > 25% (> RM 1,044M)
Tier 2: Production Segment (FPSO)					
Profit After Tax (RM 927M)*	Decrease by < than 20% (< RM 185M)	Decrease by 20% - 40% (RM 185M – RM 371M)	Decrease by 40% - 60% (RM 371M – RM 556M)	Decrease by 60% - 80% (RM 556M – RM 742M)	Decrease by > 80% (> RM 742M)
Total Revenue (RM 5,873M)*	Decrease by < than 6% (< RM352M)	Decrease by 6% - 13% (RM 352M – RM 763M)	Decrease by 13% - 20% (RM 763M – RM 1,175M)	Decrease by 20% -25% (RM 1,175M – RM 1,468M)	Decrease by > 25% (> RM 1,468M)
Total Cost (RM 4,102M)*	Increase by < than 6% (< RM 246M)	Increase by 6% - 13% (RM 246M – RM 533M)	Increase by 13% - 20% (RM 533M – RM 802M)	Increase by 20% - 25% (RM 802M – RM 1,026M)	Increase by > 25% (> RM 1,026M)
Tier 2: Marine Segment (OSV)					
Profit After Tax (RM 20M)*	Decrease by < than 20% (< RM 4M)	Decrease by 20% - 40% (RM 4M – RM 8M)	Decrease by 40% - 60% (RM 8M – RM 12M)	Decrease by 60% - 80% (RM 12M – RM 16M)	Decrease by > 80% (> RM 16M)
Total Revenue (RM 56M)*	Decrease by < than 6% (< RM 3.4M)	Decrease by 6% - 13% (RM 3.4M – RM 7.3M)	Decrease by 13% - 20% (RM 7.3M – RM 11.2M)	Decrease by 20% -25% (RM 11.2M – RM 14M)	Decrease by > 25% (> RM 14M)
Total Cost (RM 37M)*	Increase by < than 6% (< RM 2.2M)	Increase by 6% - 13% (RM 2.2M – RM 4.8M)	Increase by 13% - 20% (RM 4.8M – RM 7.4M)	Increase by 20% - 25% (RM 7.4M – RM 9.2M)	Increase by > 25% (> RM 9.2M)
Tier 2: Renewable Energy Segment					
Profit After Tax (-RM 84M)*	Increase by < than 20% (> - 17M)	Increase by 20% - 40% (RM - 17M – - RM 34M)	Increase by 40% - 60% (RM -34M – RM -50M)	Increase by 60% - 80% (RM -50M – RM -67M)	Increase by > 80% (> RM 6-7M)
Total Revenue (RM 73M)*	Decrease by < than 6% (< RM 4.4M)	Decrease by 6% - 13% (RM 4.4M – RM 9.5M)	Decrease by 13% - 20% (RM 9.5M – RM 14.6M)	Decrease by 20% -25% (RM 14.6M – RM 18.3M)	Decrease by > 25% (> RM 18.3M)
Total Cost (RM 33M)*	Increase by < than 6% (> RM 1.9M)	Increase by 6% - 13% (RM 1.9M – RM 4.3M)	Increase by 13% - 20% (RM 4.3M – RM 6.6M)	Increase by 20% - 25% (RM 6.6M – RM 8.3M)	Increase by > 25% (> RM 8.3M)



Appendix 14.3 – Detailed of Risk Impact Rating for Financial Parameters (cont'd)

Factor	Financial Impact (in RM)				
	Insignificant	Minor	Moderate	Major	Catastrophic
Tier 2: GreenTech Segment					
Profit After Tax (-RM 35M)*	Increase by < than 20% (> - 7M)	Increase by 20% - 40% (RM -7M – -RM 14M)	Increase by 40% - 60% (RM -14M – RM -21M)	Increase by 60% - 80% (RM -21M – RM -28M)	Increase by > 80% (>-RM 28M)
Total Revenue (RM 1M)*	Decrease by < than 6% (< RM 60,000)	Decrease by 6% - 13% (RM 60,000 – RM 130,000M)	Decrease by 13% - 20% (RM 130,000 – RM 200,000)	Decrease by 20% -25% (RM 200,000 – RM 250,000)	Decrease by > 25% (> RM 250,000)
Total Cost (RM 3M)*	Increase by < than 6%% (> RM 180,000)	Increase by 6% - 13% (RM 180,000 – RM 390,000)	Increase by 13% - 20% (RM 390,000 – RM 600,000)	Increase by 20% - 25% (RM 600,000 – RM 750,000)	Increase by > 25% (> RM 750,000)
Tier 3: Production segment (FPSO) – Ghana (YPWAL)					
Profit After Tax (RM 29M)*	Decrease by < than 20% (< RM 6M)	Decrease by 20% - 40% (RM 6M – RM 12M)	Decrease by 40% - 60% (RM 12M – RM 17M)	Decrease by 60% - 80% (RM 17M – RM 23M)	Decrease by > 80% (> RM 23M)
Total Revenue (RM 252M)*	Decrease by < than 6% (< RM 15.1M)	Decrease by 6% - 13% (RM 15.1M – RM 32.8M)	Decrease by 13% - 20% (RM 32.8M – RM 50.4M)	Decrease by 20% -25% (RM 50.4M – RM 63M)	Decrease by > 25% (> RM 63M)
Total Cost (RM 174M)*	Increase by < than 6% (< RM 10.4M)	Increase by 6% - 13% (RM 10.4M – RM 22.6M)	Increase by 13% - 20% (RM 22.6M – RM 34.8M)	Increase by 20% - 25% (RM 34.8M – RM 43.5M)	Increase by > 25% (> RM 43.5M)
Tier 3: Production Segment (FPSO) – Nigeria (YOPWAL)					
Profit After Tax (RM 3M)*	Decrease by < than 20% (< RM 600,000)	Decrease by 20% - 40% (RM 600,000 – RM 1.2M)	Decrease by 40% - 60% (RM 1.2M – RM 1.8M)	Decrease by 60% - 80% (RM 1.8M – RM 2.4M)	Decrease by > 80% (>RM 2.4M)
Total Revenue (RM 113M)*	Decrease by < than 6% (< RM 6.8M)	Decrease by 6% - 13% (RM 16.8M - RM 14.7M)	Decrease by 13% - 20% (RM 14.7M – RM 22.6M)	Decrease by 20% - 25% (RM 22.6M – RM 28.3M)	Decrease by > 25% (>RM 28.3M)
Total Cost (RM 99M)*	Decrease by < than 6% (< RM 5.9M)	Decrease by 6% - 13% (RM 5.9M - RM 12.9M)	Decrease by 13% - 20% (RM 12.9M – RM 19.8M)	Decrease by 20% - 25% (RM 19.8M – RM 24.8M)	Decrease by > 25% (>RM 24.8M)
Tier 3: Production Segment (FPSO) – Miri (YLOSB)					
Profit After Tax (RM 43M)*	Decrease by < than 20% (< 8.6M)	Decrease by 20% - 40% (RM 8.6M – RM 17.2M)	Decrease by 40% - 60% (RM 17.2M – RM 25.8M)	Decrease by 60% - 80% (RM 25.8M – RM 34.4M)	Decrease by > 80% (>RM 34.4M)
Total Revenue (RM 107M)*	Decrease by < than 6% (< RM 6.4M)	Decrease by 6% - 13% (RM 6.4M - RM 13.9M)	Decrease by 13% - 20% (RM 13.9M – RM 21.4M)	Decrease by 20% - 25% (RM 21.4M – RM 26.8M)	Decrease by > 25% (>RM 26.8M)
Total Cost (RM 51M)*	Decrease by < than 6% (< RM 3M)	Decrease by 6% - 13% (RM 3M - RM 6.6M)	Decrease by 13% - 20% (RM 6.6M – RM 10.2M)	Decrease by 20% - 25% (RM 10.2M – RM 12.8M)	Decrease by > 25% (>RM 12.8M)

Source: (*) Yinson Holdings Berhad FY2023 Actuals (unaudited)

Remarks: The risk parameter is subjected to review by the Management in the next risk assessment.



Appendix 14.4 – Detailed of Risk Impact Rating for Non-Financial Parameters

Factor	Impact				
	Insignificant	Minor	Moderate	Major	Catastrophic
Risk Impact Description	<ul style="list-style-type: none"> Minimal/ negligible disruption. Minimal effort for correction 	<ul style="list-style-type: none"> Limited disruption Recoverable/ manageable through routine procedures. 	<ul style="list-style-type: none"> Noticeable to material disruptions Management intervention is required for recovery/correction. 	<ul style="list-style-type: none"> Significant disruptions Management intervention and material resources may be required for recovery/correction. 	<ul style="list-style-type: none"> Disastrous/ irreversible disruption with long term impact Full recovery is uncertain, requires immediate comprehensive response and substantial resources.
Strategic	<ul style="list-style-type: none"> No impact to any strategic initiatives 	<ul style="list-style-type: none"> Slight delay or adjustment in strategy execution 	<ul style="list-style-type: none"> Notable impact on strategic goal achievement; requires strategic alignment 	<ul style="list-style-type: none"> Significant derailment of strategy; major strategic overhaul required 	<ul style="list-style-type: none"> Fundamental threat to strategic foundations; potential failure in achieving core objectives
Environment and Sustainability	<ul style="list-style-type: none"> Minimal impact Quick and easily recoverable 	<ul style="list-style-type: none"> Minor impact Requires adjustment to practices or minor investments for correction 	<ul style="list-style-type: none"> Moderate impact not affecting ecosystem Potential non-compliance and requires dedicated efforts to address 	<ul style="list-style-type: none"> Significant impact affecting ecosystem Long-term sustainability compromised 	<ul style="list-style-type: none"> Major environmental damage, causing long-term ecological harm and potentially affecting the business' ability to operate.
Operations	<ul style="list-style-type: none"> Negligible delay or error Easy recovery to resume operations with no impact to production or project targets 	<ul style="list-style-type: none"> Minor disruption to specific tasks or processes with noticeable drop in function effectiveness Resolvable with negligible impact to production, operation or project targets 	<ul style="list-style-type: none"> Notable disruption to key processes or activities Requires dedicated resources for recovery with potential impact on production or project targets 	<ul style="list-style-type: none"> Major disruption to operations or project completion Requires significant resources and potentially impacting core business functions 	<ul style="list-style-type: none"> Major disruption or failure of critical operations, potentially leading to negative project returns and/or abandonment of the project



Factor	Impact				
	Insignificant	Minor	Moderate	Major	Catastrophic
Compliance and Regulatory	<ul style="list-style-type: none"> No litigation consequences. Issuance of advice letter. 	<ul style="list-style-type: none"> Issuance of reprimand / warning letter. Minimum fine. 	<ul style="list-style-type: none"> Issuance of public reprimand / warning letter. Moderate fine. 	<ul style="list-style-type: none"> Multiple issuances of public reprimands / warning letters. Heavy fines. Suspension of share. 	<ul style="list-style-type: none"> Closure of operations Jail sentence for directors
Health & Safety	<ul style="list-style-type: none"> First aid case / Case with no medical treatment 	<ul style="list-style-type: none"> Minor temporary disability requiring sick leave of not more than 4 days 	<ul style="list-style-type: none"> Minor permanent disability requiring medical attention with potential LTI case. 	<ul style="list-style-type: none"> Lost Time Incident case with single fatality or severe permanent disability 	<ul style="list-style-type: none"> Lost Time Incident case with multiple fatalities
Technology and Cybersecurity	<ul style="list-style-type: none"> Negligible downtime No data/asset loss 	<ul style="list-style-type: none"> Isolated event impacting specific non-critical infrastructure Insignificant data security breach Requires IT response 	<ul style="list-style-type: none"> Significant system failures or data security breaches Requires major IT overhaul 	<ul style="list-style-type: none"> Major outage or data security breach impacting core business functions, data confidentiality Requires substantial reinvestment and other IT resources for recovery 	<ul style="list-style-type: none"> Catastrophic system failure or widespread data breach causing long-term disruptions to core business functions



Appendix 14.4 – Detailed Risk Impact Rating for Non-Financial Parameter (cont'd)

Factor	Impact				
	Insignificant	Minor	Moderate	Major	Catastrophic
Reputation	<ul style="list-style-type: none"> • Insignificant negative perception • Quickly manageable with minimal effort 	<ul style="list-style-type: none"> • Small-scale negative perception or by small group • Requires targeted communication or compensation 	<ul style="list-style-type: none"> • Moderate damage to public image • Requires stakeholder management and significant apologetic/ PR efforts • Minimal impact to long-term trust 	<ul style="list-style-type: none"> • Significant reputational damage, loss of trust, customer churn and termination of partnerships • Requires public engagement, apologetic efforts and significant compensation • Share price moderately affected 	<ul style="list-style-type: none"> • Reputational crisis with potentially irreparable damage • Termination of contracts by long-term strategic business partners • Boycotts and significant drop in share price
Bribery and Corruption	<ul style="list-style-type: none"> • No adverse publicity or ministerial involvement • No conflicts with any engaged stakeholders • Breach of internal process and controls 	<ul style="list-style-type: none"> • Some adverse publicity • Minor loss of stakeholder confidence • Internal review of existing policies and practices instigated • Breach of guidelines and SOP 	<ul style="list-style-type: none"> • Substantial adverse publicity • Loss of some stakeholder confidence • Risk event requires Management response • Breach of ABAC Policy (<i>i.e. ISO37001</i>) 	<ul style="list-style-type: none"> • Adverse national media reports on failings, inefficiency or inadequacy • Serious loss of stakeholder confidence • Serious consequences to Senior Management which may lead to penalty / imprisonment • Breach of laws and regulations resulting in penalty (<i>i.e. List of acts and legal reference in Appendix 14.6</i>) 	<ul style="list-style-type: none"> • Intense public, political and media scrutiny / criticism evidenced by front-page headlines, adverse international media and reports and / or sustained television coverage • Complete loss of stakeholder confidence • Board of Director penalty / imprisonment • Breach of laws and regulations resulting in criminal penalty (<i>i.e. List of acts and legal</i>



Title : Enterprise Risk Management (ERM) Policy Revision : 08
Statement & Framework

Document No : YHB-RC-CG-PP-0004

Date : 1-Mac-2024

					<i>reference in Appendix 14.6)</i>
--	--	--	--	--	--



Appendix 14.5 – Risk Matrix Descriptions

Risk Heat Map			Risk Impact				
			Insignificant	Minor	Moderate	Major	Catastrophic
			1	2	3	4	5
Risk Likelihood	Almost Certain	5	Medium (5)	Medium (10)	High (15)	Critical (20)	Critical (25)
	Likely	4	Low (4)	Medium (8)	High (12)	High (16)	Critical (20)
	Possible	3	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
	Unlikely	2	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium (10)
	Rare	1	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

Appendix 14.6 – List of Acts and Legal References

Malaysia

- Federal Constitution
- Malaysian Anti-Corruption Commission Act 2009 (Act 694)
- Anti-Corruption Act 1997 (Act 575)
- Penal Code (Act 574)
- Criminal Procedure Code (Act 593)
- Courts of Judicature Act (Act 91)
- Evidence Act 1950 (Act 56)
- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613)
- Witness Protection Act 2009 (Act 696)
- Whistle blower Protection Act 2010 (Act 711)
- Criminal Procedure (Rates of Payment to Witnesses) Rules 2011
- Appointment of Lock-Up To Be A Place of Confinement (Gazette)
- Malaysian Anti-Corruption Commission (Amendment) Act 2018 (Act A1567)

Singapore

- Prevention of Corruption Act, Chapter 241.
- Penal Code, Chapter 224.
- Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act, Chapter 65A.
- Organized Crime Act (Act No. 26 of 2015) - stipulates that assets could be seized where these are found to be proceeds of corrupt activity.

Ghana

- Criminal Offences Act, 1960 (Act 29);
- Companies Code, 1963 (Act 179);
- Whistle Blower Act 2006 (Act 720);
- Customs Act, 2015 (Act 891);
- Public Financial Management Act, 2016 (Act 921);



Title : Enterprise Risk Management (ERM) Policy
Statement & Framework

Revision : 08

Document No : YHB-RC-CG-PP-0004

Date : 1-Mar-2024

- Representation of the People Law (PNDCL 284);
- Audit Service Act, 2000 (Act 584);
- Government Contracts (Protection) Act, 1979 (AFRCD 58);
- Economic and Organized Crime Office Act, 2010 (Act 804);
- Constitution of the Republic of Ghana 1992;
- Ghana is also a signatory to the following conventions:
 - United Nations Convention against Corruption; and
 - the African Union Convention on Preventing and Combating Corruption.



Nigeria

- Corrupt Practices and Other Related Offences Act 2000, Act No.5 Laws of the Federation of Nigeria.
- Economic and Financial Crimes Commission (Establishment) Act 2003 (Chapter E1, LFN 2004).
- Code of Conduct for Public Officers, Fifth Schedule to the Constitution of the Federal Republic of Nigeria 1999
- Criminal Code Act (Chapter C38, LFN 2004) - applicable to the Southern part of Nigeria.
- Penal Code - applicable to the Northern part of Nigeria.
- Advance Fee Fraud and Other Related Offences Act 2006.
- Nigeria is also a signatory to the following conventions:
 - African Union Convention on Preventing and Combating Corruption;
 - United Nations Convention Against Corruption; and
 - United Nations Convention Against Transnational Organized Crime.

Norway

- Norwegian Penal Code
- Anti-Money Laundering and Terrorist Financing Act
- Norwegian Labour Law
- Political Parties Act
- Working Environment Act
- Public Procurement Act
- Public Administration Act
- EEA Competition Act
- Personal Data Act
- Limited Liability Companies Act
- Securities Trading Act
- Accounting Act
- Book-keeping Act
- Political Parties Act
- Civil Service Act
- Heath Personnel Act
- EU Procurement Directives - establishes conditions for mandatory exclusion of economic operators who have been convicted of financial crimes, including corruption.
- Norway is also a signatory to the following conventions:
 - OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1997);
 - United Nations Convention Against Corruption (UNCAC);
 - The Council of Europe Civil Law Convention on Corruption (1999); and
 - The Council of Europe Criminal Law Convention on Corruption (1999).



Brazil

- Brazilian Clean Company Act (Law 12846/2013)
- Brazilian Penal Code (Decree-Law 2848/1940)
- Administrative Improbity Law (Law 8429/1992)
- Decree 8420/2015
- Ordinances 909/2015 and 910/2015 of the Ministry of Transparency, Monitoring and Control (previously the CGU)
- Law 13608/2018
- Decree 10153/2019
- Anti-Money Laundering Law (Law 9613/1998 and 12683/2012).
- Procurement Law (Law 8666/1993)
- Conflict of Interest Law (Law 12813/2013)
- Crimes of Responsibility Law (Law 1079/1950 and Decree 201/1967)
- Clean Records Law (Complementary Law 135/2010)
- Anti-Trust Law (Law 12529/2011)
- Anticrime Law (Law 13.964/2019)
- Decree 4081/2002
- Law 13869/2019
- Normative Instructions of CGU 01/2015 and 02/2015
- There are also norms of the Public Ethics Commission and codes of conduct and ethics and manuals that apply to public officials
- Brazil is also a signatory to the following conventions:
 - the Inter-American Convention against Corruption (1996)
 - the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1997)
 - the United Nations Convention against Transnational Organized Crime (2000)
 - the United Nations Convention against Corruption (2003)

Netherlands

- Dutch Criminal Code
- Code of Criminal Procedure
- The Netherlands is also a signatory to the following conventions:
 - the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1997)
 - the United Nations Convention Against Corruption (2003)