ORKIM SDN BHD

RISK MANAGEMENT
POLICY AND PROCEDURES

DOCUMENT TITLE	**RISK MANAGEMENT POLICY AND PROCEDURES**		
DOCUMENT REF	**ORKIM/RISK/P&P/01/00/25**		
OWNER	RISK, AUDIT AND COMPLIANCE DEPARTMENT		
ISSUE	1	ISSUE DATE	15 MAY 2025
REVISION	0	REVISION DATE	NIL
PREPARED BY	SYED EFFIZAN (HEAD OF RISK, AUDIT AND COMPLIANCE)	SIGNATURE	
		DATE	
REVIEWED BY	TAHIRAH MOHD NOR (CHIEF FINANCIAL OFFICER)	SIGNATURE	
		DATE	
APPROVED BY	CHEAH SIN BI (CHIEF EXECUTIVE OFFICER)	SIGNATURE	
		DATE	
FINAL APPROVED BY	(NAME) (CHAIRMAN, BOARD RISK AND AUDIT COMMITTEE)	SIGNATURE	
		DATE	

TABLE OF CONTENTS

POLICY

STANDARD OPERATING PROCEDURES

SECTION 1 – POLICY STATEMENT AND OBJECTIVE

The Risk Management Policy and Procedures is developed to guide Risk, Audit and Compliance ("RAC") Department in providing the services of management of risk faced by Orkim Sdn Bhd and its group of companies ("Orkim" or "the Group"). The Policy and Procedures addresses the following:

a) Recognizing that risk is an integral component of business and is characterized by both threat and opportunity. As such, the Company is committed to foster a risk-aware culture in all decision making.

b) Consider weighing business decisions against the philosophy that business risks would be incurred if the associated rewards are expected to enhance the Group's shareholders value.

c) Proactively and effectively manage all risks and ensure that risks which may have a significant impact upon the Group are identified and treated.

d) Providing reasonable assurance to the Group's shareholders that the probability of attaining its objectives will be enhanced by the establishment and maintenance of an appropriate enterprise-wide risk management framework.

e) Ensuring all levels of personnel within the Group understand their roles and responsibilities in relation to risk management.

f) Ensuring legal and regulatory compliance, as well as preventing and detecting fraud/ irregularities to the extent possible.

g) That the Group will communicate and provide the necessary resources, structures, system and training to ensure this P&P is understood, implemented and maintained at all levels.

SECTION 2 - CIRCULATION AND REVIEW

The Policy and Procedures shall be reviewed at least annually. RAC Department shall be responsible for the administration, interpretation and application of this Policy and Procedures. This Policy and Procedures shall be made available to all Orkim's employees.

SECTION 3 – APPLICATION

The Policy and Procedures shall apply to all directors, management, employees and contractors employed or working on board Orkim's vessels and in Orkim's offices ashore, also requiring the same standards to be followed by our supplier, outsourcing companies, contractors, customers and other value chain partners.

The Policy and Procedures shall be read in conjunction with the Orkim approved Limits of Authority ("LOA") and any associated provision in the Orkim Management Procedure Manual ("MPM"). In the event of a conflict between this Policy and Procedures and the MPM, this Policy and Procedures shall govern.

SECTION 4 – INDEPENDENCE

To foster an appropriate level of independence, as well as effective reporting and communication, the Risk Management function of the RAC Department reports functionally to the Board Risk and Audit Committee ("BRAC") and administratively to the Risk Management Committee ("RMC") and to the Chief Executive Officer ("CEO").

The RMC is chaired by the CEO with members comprised of:

a) Chief Financial Officer ("CFO")
b) Head of RAC
c) Head of Marine Operation
d) Head of Safety and Quality/ Designated Person Ashore ("DPA")
e) Head of Technical
f) Head of Procurement
g) Head of Business Development
h) Head of Commercial
i) Head of Chartering
j) Head of Fleet Personnel
k) Head of Human Resources and Administration
l) Head of Legal and Communications
m) Head of Information Technology and Systems (Cybersecurity)
n) Head of ESG/ Sustainability (where available)

SECTION 5 – ROLES AND RESPONSIBILITIES

The table below summarizes the key risk management authority, roles and responsibilities:

Structure	Authority, roles and responsibilities
Board Risk and Audit Committee ("BRAC") or the Board of Directors ("Board")	a) Retains overall risk management responsibility by providing oversight and representing shareholders' and the Group's interests in managing risks by formalizing a sound enterprise-wide risk management framework to: – Identify and evaluate risks affecting the Group – Manage and mitigate risks identified, by implementing effective and efficient control measures and treatment plans – Report and communicate measures deployed to manage and mitigate those risks identified – Monitor and review residual risks periodically, including measures deployed to manage and mitigate those risks identified. b) Sets the "tone-at-the-top" to drive a risk-aware culture throughout the organization. c) Embeds risk management in all aspects of the Group's activities. d) Periodically reviews and approves the risk parameter and appetite of the Group, which are aligned with the objectives and strategies, and communicating them appropriately. e) Review and approve the Orkim Group Risk Management Policy, including proposed changes thereof. f) Periodically deliberates and approves key risk matters/ issues, including overall risk profile of the Group. g) Periodically reviews the risk management framework, process, responsibilities and assessing whether they provide reasonable assurance that risks are managed within tolerable ranges.

Structure	Authority, roles and responsibilities
Chief Executive Officer ("CEO")	a) Overall "Risk Champion" entrusted by the BRAC/ Board to manage and mitigate all key risks within the organization with a view to enhance shareholders' value and safeguard the assets of the Group. b) Designs and implements a sound enterprise-wide risk management framework in accordance with the Group's strategic vision and overall risk parameter and appetite, which considers compliance with legal and regulatory requirements, as well as considering measures taken to deter fraud/ irregularities that may occur within the Group. c) Allocates resources and delegates tasks to ensure effective and efficient risk management is practiced within the Group. d) Risks are considered, evaluated, mitigated and monitored for all key business proposals/ investments, procurement and decisions made. e) Embeds sound risk management practices in strategy formulation. f) Identifies changes to risks or emerging risks, acts as appropriate, and brings this to the attention of the BRAC/ Board. g) Implements an effective system of internal controls/ treatment plans to mitigate risks to an acceptable level within the organization.

Risk Management Committee ("RMC")	a) The RMC at the management level is established to support the CEO in identifying, assessing and mitigating risks that may impact the company's operations, financial stability, and strategic objectives. The RMC shall: ▪ Identify and mitigate risks affecting business operations, including financial, regulatory, cybersecurity and ESG-related risks. ▪ Ensure adherence to regulatory requirements and internal risk control measures. ▪ Oversee the development of contingency plans for risk events (business continuity and crisis management). ▪ Promote risk awareness and accountability across all management levels. ▪ Provide quarterly risk reports to the CEO and relevant stakeholders. b) RMC's secretariat to be appointed by the CEO (the Company Secretary or Head of RAC) c) The Committee shall meet at least quarterly and the quorum for meetings shall be six (6) members, including the CEO. d) The Chairperson may call for additional meetings as necessary. e) Decisions shall be made by majority vote, with the CEO holding a casting vote in case of a tie. f) RMC shall maintain minutes of each meeting, which shall be circulated to all Divisional/Departmental Heads.
Divisional and Departmental Heads	a) Retains overall ownership to manage and mitigate all key risks within their respective area of responsibility, i.e. "Risk Owner". b) Oversees and participates in the implementation of the enterprise-wide risk management framework within their respective area of responsibility, including compliance with the Risk Management Policy and Procedures. c) Considers and evaluates risks, including the appropriate treatment/ action plans developed to mitigate those risks to an acceptable level for all key operations, business/ investment proposals/ plans, procurement and proposal papers.

Structure	Authority, roles and responsibilities
Divisional and Departmental Heads (cont'd)	d) Ensures risk management practices and principles are considered upon developing departmental/divisional procedures. e) Escalates high risk areas and proposed controls/ risk treatment plan within their capacity to the BRAC/ Board, CEO and/ or RAC Department as appropriate. f) Periodically monitors and reports the status of key risks to the CEO and RAC Department, including the implementation of proposed controls/ risk treatment plan within their respective areas of responsibility. g) Ensure that agreed upon risk treatment plans are implemented on a timely basis and the system of internal control established and maintained within their respective areas of responsibility are working effectively and efficiently.
All Orkim Employees	a) Directly responsible for the day-to-day management and mitigation of key risks within their respective areas of responsibility. b) Actively participates in the implementation of the enterprise-wide risk management framework within their respective areas of responsibility, including compliance with the Risk Management Policy and Procedures. c) Escalates high risk areas and proposed controls/ risk treatment plan within their capacity to their respective Divisional/Departmental Head.
Risk, Audit and Compliance ("RAC") Department	a) The "Risk Facilitator" that coordinate and streamline the identification, analysis, evaluation, reporting, treatment and monitoring of all key risks affecting the Group. b) Facilitate the development and maintenance of an enterprise-wide risk management framework. c) Coordinate with the development of risk parameter and appetite, which are aligned with the strategies/ business plan of the Group. d) Focal point to guide the Group on governance, risk and controls matters and issues. e) Promote a "risk-aware" culture within the Group by conducting briefings/ trainings/ workshops on latest risk management updates and initiatives. f) Review all key business/ investment proposals/ plans,

	procurement and proposal papers to ensure that management has considered and evaluated risks, including the appropriate treatment/ action plans developed to mitigate those risks to an acceptable level. g) Review all operating procedures developed by all Divisions and Department to ascertain if good risk management practices and controls are embedded within those procedures developed. h) Facilitate with the monitoring process on the implementation of risk treatment plans by the respective risk owners to mitigate risks to an acceptable level within the organization. i) Periodically highlights/ reports improvement opportunities and non- adherence to the enterprise-wide risk management framework to the BRAC/ Board and CEO. j) Creates a bridge between risk management and internal audit to enable an effective system of internal controls/ treatment plans implemented by management to mitigate risks to an acceptable level within the organization.

SECTION 6 – STANDARD OPERATING PROCEDURES

6.1 Purpose

The purpose of the Enterprise-wide Risk Management ("ERM") procedure is to:

a) Identify and formalize in a systematic manner the scope and responsibilities of the Risk Management function of the RAC Department as well as the various Divisions/Departments of the Group.
b) Facilitate the integration of risk management into day-to-day business activities and practices.
c) Provide guidance on ERM principles to all Divisional/Departmental Heads to govern the actions of their subordinates pertaining to risks.
d) Provide assurance to the BRAC that a sound risk management and internal control system are in place and in conformance with globally accepted risk management standards and practices.

6.2 Scope

The ERM procedure is designed to provide consistent guidance to the RAC Department to embed the ERM process across all functions and standardize the understanding and application of ERM within Orkim Group. This procedure manual is aligned with the risk management best practices as promulgated by the Enterprise Risk Management – Integrated Framework 2004 by Committee of Sponsoring Organizations of the Treadway Commission ("COSO ERM Framework").

6.3 Independence

The RAC Department does not set the risk appetite or make decisions on risk responses and implement these responses on behalf of Management. Management remains primarily responsible and accountable for the identification, assessment and treatment of risk. In addition, the RAC Department does not develop and implement procedures or systems (i.e. other than procedures relating to Risk Management) or being engaged in operational or processing functions.

6.4 Definition of Risk

Risk is defined as potential events or an uncertainty that if it occurs it could adversely affect the Group, in the following:

a) Adverse value to the Group's shareholder and other stakeholders
b) Inability to achieve objectives and implementation of business strategies
c) Erosion of image, reputation and branding in the industry that the Group operates

6.5 Definition of Enterprise-wide Risk Management ("ERM")

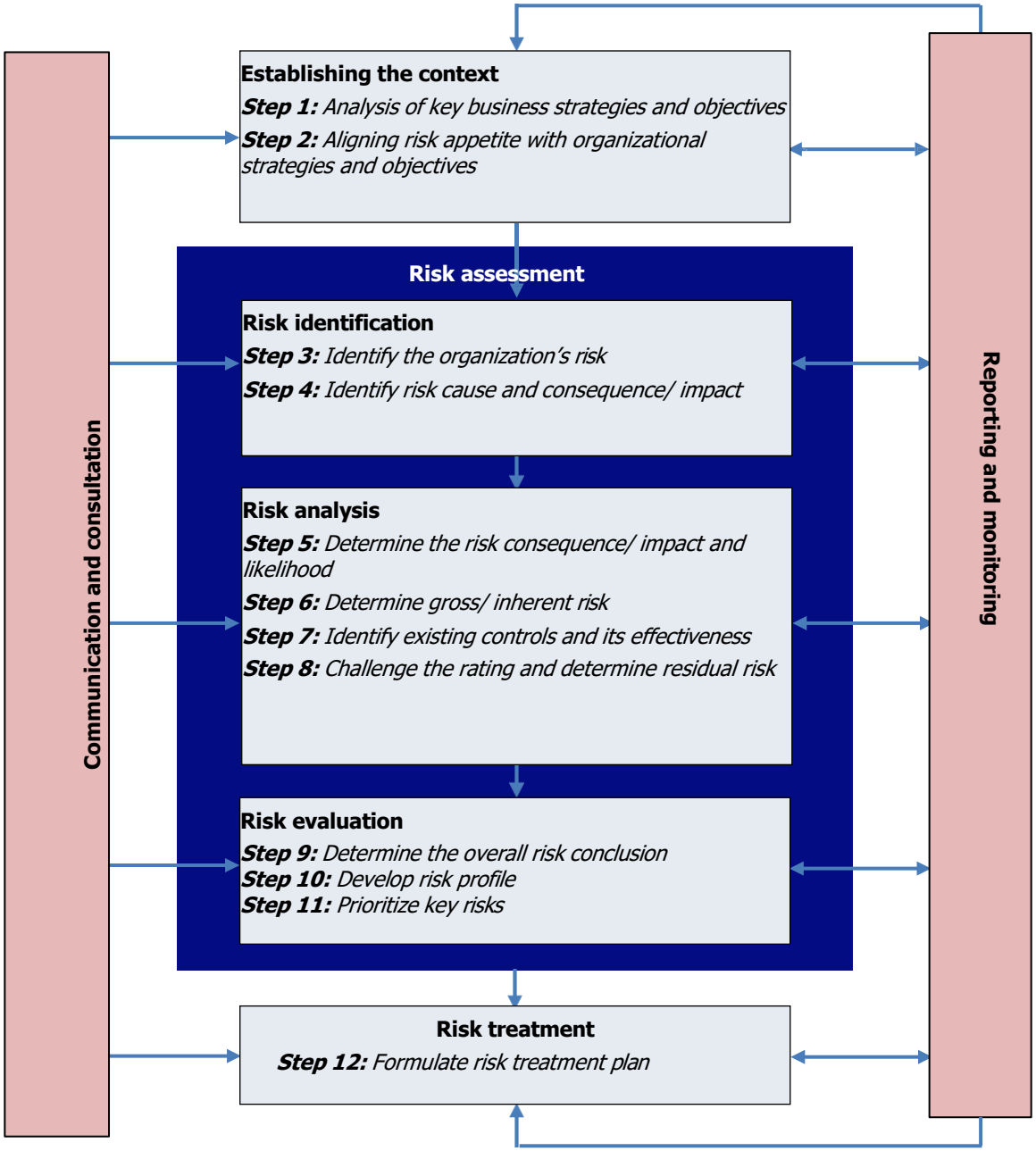
ERM is a structured and disciplined approach, aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing key business risks that an organization faces as it creates value. This process is designed to identify potential events that may affect the organization and manage key business risks to be within the organization's risk appetite to provide a reasonable assurance regarding the achievement of its objectives.

ERM shall be a core management competency that incorporates a well-structured systematic process to identify key business risks and lessen their impact and likelihood on the organization. This process should be adopted by everyone within an organization, i.e. the Board, management and employees. This involves the following core elements:

a) The identification of key business risks
b) The measurement of the identified key business risks
c) The control or the way the key risks are managed
d) The monitoring and communicating of key business risks in a way that will enable the organization to minimize losses and maximize opportunities

The benefit of effective risk management in an organization is that it enables the decision makers of an organization to better forecast and quickly adapt to the changing demands that are placed upon the organization. It also means that the organization is less likely to be surprised by some external events that warrant for significant change.

6.6 Snapshot of ERM Process



6.7 Establishing the Context

Step 1: Analysis of key business strategies and objectives

1. Key business strategies and objectives are set at the strategic level, establishing a basis for operations, reporting and compliance objectives. Every organization faces a variety of risks from external and internal sources, and a precondition to effective ERM is the establishment of these strategies and objectives. Objectives are aligned with the organization's risk appetite and external and internal factors which drive risk need to be considered in analyzing key business strategies and objectives. Examples of external factors may include:

    a) Political - Election of government officials with new political agendas or new laws and regulations i.e. taxes, access to domestic/foreign market
    b) Legal - Regulatory breach, resulting in court settlement, temporary suspension of works, reprimand, censure, fines, high profile litigation cases
    c) Economic - Price movement, capital availability, barriers to competitive entry
    d) Environment – Adverse weather conditions, carbon emissions
    e) Social – Safety and human resources issues
    f) Technological – New means of electronic based operating system and technology-based services, data security

2. Examples of internal factors may include:

    a) Process – Process changes without adequate change protocols, process execution errors, ineffective and inefficient work process, outsourcing functions with inadequate oversight
    b) Employees – Workplace accidents, fraudulent activities
    c) Infrastructure – Increasing capital allocation on preventive maintenance, reducing vessel downtime and improving customer satisfaction
    d) Technology- Security breaches

3. RAC Department would assist Divisional/Departmental Heads to identify and analyze key business strategies and objectives of the Group as a whole, as well as the related processes/ activities. This includes strategic analysis of critical success factors/ enablers of key business strategies and objectives, key performance indicators, process/ activities inputs and outputs, business/ development plans, key financials, feasibility studies, market research/ studies, competitor analysis, budget, key project milestone, rules and regulations affecting the Group, etc.

4. The information derived from this process is then used to guide the Group to determine its risk parameter and appetite levels, as well as to begin the process of risk identification within their division/department.

Step 2: Aligning risk parameter and appetite with organizational strategies and objectives

1. Risk parameter and appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. It reflects the organization's risk management philosophy and in turn influences the organization's culture and operating style.

2. Different strategies will expose the organization to different levels of risk, and ERM, applied in strategy setting, enables the management to select strategies consistent with the organization's risk parameter and appetite (defined by risk consequence/ (measured in terms of financial and non-financial factors) and risk likelihood (probability of risk occurrence within the next 12 months).

3. The following would also be considered when developing the risk parameter and appetite:

    a) The Group's current and future business and development plans
    b) The Group's Limits of Authority ("LOA")
    c) People, processes and systems of the Group
    d) Risk parameter and appetite of other reputable competitor within the industry

4. The organizational risk parameter and appetite will be proposed by the CEO to the BARC/ Board, for deliberation and approval, accordingly. A sample risk parameter and appetite is shown in **Appendix 1.**

6.8 Risk Assessment

The risk assessment process involves risk identification, risk analysis and risk evaluation. The risk assessment process is further elaborated in *Steps 3 to 11* below.

Management identifies potential risks, which if they occur, will affect the Group adversely to successfully implement its strategies and objectives. By linking risk with the strategies and objectives, this will ensure that the risk identification process focuses on those uncertainties that matter, rather than being distracted and diverted by irrelevant uncertainties.

Accordingly, risks would require management's assessment and response. When identifying a risk, it involves the determination of the risk source i.e. external and internal factors, as well as the risk's cause(s) and potential consequence/ impact. In identifying a risk, this would require management to consider historical data, theoretical analysis, informed and expert opinions and stakeholders' needs, where appropriate.

Step 3: Identify the organization's risk

1. A risk is an incident or occurrence emanating from internal or external sources that affects the implementation of strategies and achievement of objectives negatively. In identifying a risk, a myriad of external and internal influencing factors which drive risk need to be considered i.e. the risk source. As a guide to identify risk, reference can be made to *Step 1* to identify the major contributing factors of risk faced by an organization.

2. Once the major contributing factors are identified, management can identify the risk and consider their significance and focus on risks that can affect the implementation of strategies and achievement of objectives. This would assist management to ascertain if all key risks affecting the Group have been identified.

3. Management can consider risk identification on division/ department/ vessel/ projects e.g. Commercial, Chartering, Technical, Marine Operation, Marine Safety and Quality, Procurement, Fleet Management, Human Resources, Information Technology and Finance etc.

4. In the risk identification process, management could consider the following questions to assist in the identification of organizational risks:

    a) What could go wrong?
    b) What problems are we trying to mitigate?
    c) How can we identify or detect errors?

d) Could fraud or abuse occur?
e) Could there be fines and penalties imposed by regulators?
f) Does this activity depend on the support from third parties and what happens if the Group does not obtain the desired outcome from the support provided by third parties?

5. Upon identifying a key business risk, it would be placed within 4 broad risk categories (Strategic, Operational, Financial, Project) which are defined as follows:

Broad risk category	Description
Strategic	Strategic risks are those risks having a direct/ indirect impact on the Group's objectives, that are aligned with and support the Group's mission. This may also include risks that are external or internal to the Group but have a significant impact on its strategic decisions or activities. Notwithstanding the above, if an individual or a group of interrelated operational and project risks carries a significant impact to the Group's going concern or strategy, it can be considered as a strategic risk. Accountability for managing strategic risks therefore rests with the Board/ BRAC and CEO.
Operational	Operational risks are inherent in the ongoing activities within the different functions of the Orkim Group which result from breakdowns/weaknesses in internal procedures, people and systems as well as from external events such as physical or environmental factors. Accountability for managing operational risks therefore rests with the CEO, who may delegate it to Divisional/Departmental Heads.
Financial	Financial risks are associated with the probability of loss inherent in financial management and financing methods which may impair the Group's cash flow, the ability to provide adequate return, meet financial obligations and attainment of loans. Accountability for managing financial risks therefore rests with the CEO who may delegate it to the Chief Financial Officer ("CFO") and other related Divisional/ Departmental Heads.
Project (New building, vessel acquisition, docking etc.)	These are risks associated with projects that are of a specific, normally short-term to medium-term nature (i.e. approximately not more than 3 years) and are frequently associated with new vessel building, docking exercise, vessel acquisitions etc. Accountability for managing project risks therefore rests with the Divisional/Departmental Heads.

6. This enables risks to be aggregated and analyzed with a view to identifying a group of key risks which may have a significant impact on the Group (during the Risk Evaluation stage). This in turn would enable the management to focus its efforts and resources to mitigate those risks identified effectively and efficiently.

7. Management would also consider the risk status (i.e. active, inactive, closed or emerging) of the identified risk based on the following criteria:

Risk status	Definition
Active	Risk is current or foreseen to happen in the short-term (i.e. within 12 months upon risk identification/ update).
Inactive	Risk taken on by the Group is foreseen to happen in the medium-term or long term (i.e. more than 12 months upon risk identification).
Closed/ Terminated	Risk is no longer valid or relevant i.e. to be removed from the risk profile/ register.

8. This prepares management in advance to develop relevant and appropriate action plans for future risks and enables monitoring of risk movement within the risk profile and/ or risk register.

Step 4: Identify cause and consequence/ impact

1. To support the identified risk, management would be required to identify the cause(s) which may trigger the risk event, as well as the area of which the risk impacts the Group. The aim of this step is to generate a comprehensive and well-supported list of risks based on those events that might prevent, degrade, accelerate or delay the achievement of the Group's strategy and objective.

2. Understanding the risk cause enables management to influence the risk before they occur (i.e. change the likelihood of occurrence and consequence/ impact). In determining the cause(s), the external and internal influencing factors stipulated in *Step 3* should be taken into consideration to assist in the determination of the trigger events for the risk to arise.

3. Consequence/ impact is the effect/ undesirable outcome of an event (financial or non-financial) that would occur if the risk crystallized. In determining the consequence/ impact of risk, the possible cause(s) and adverse scenario(s) which leads to the risk event should be considered. A risk may have one or several consequence/ impacts.

4. Method to separate risks from their causes and consequences/impact via a three-part structure "risk statement" i.e. As a result of <Definite Cause>, <Uncertain Event> may occur, which would lead to <Effect on Business Objective(s)>

6.9 Risk Analysis

Risk analysis allows an organization to consider the extent to which risks have an impact on the achievement of the organization's strategies and objectives. Management analyses risks from 2 perspectives, consequence/ impact and likelihood, and normally uses a combination of qualitative and quantitative methods. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when sufficient credible data required for quantitative assessments is not practically available or obtaining and analyzing such data is not cost-effective. Quantitative assessment techniques typically bring more precision and are used in complex and sophisticated activities to supplement qualitative techniques.

The negative consequences/ impacts of risks should be examined across the organization. Subsequently, risks are analyzed both at gross (inherent) and residual (after considering effectiveness of existing controls) levels.

Step 5: Determine the risk consequence/ impact and likelihood

1. In this process, management analyses the identified risk to develop an understanding of the risk, as well as determining the magnitude of risk. This is expressed in terms of risk consequence/ impact and likelihood. The activities carried out from "Establishing the Context" and "Risk Identification" processes are further analyzed in the "Risk Analysis" process to determine the risk consequence/ impact and likelihood.

2. In determining and *level of consequence/ impact* of each identified risk, Management shall consider the following questions in the event the risk crystallizes:

   a) Could the risk be reasonably quantified against the Group's current shareholders' fund?
   b) Would it affect the going concern of the Group?
   c) Would it have any adverse financial implications i.e. impact to cash flows and earnings?
   d) What sort of adverse image and reputation damage would the Group sustain?
   e) How severe would the day-to-day business operations of the Group be affected?
   f) To what extent would customers be dissatisfied with the Group's service levels?
   g) What health and safety issues would the Group encounter, internally and externally?
   h) How would this impact on the morale and productivity of employees within the Group?
   i) Exposure to the Group in the event of breaches with regulations (i.e. imposition of fines, penalties, public reprimands, etc.)?

   The answers thereof would be analyzed and mapped against the risk parameter and appetite developed (as shown in **Appendix 1- Impact Rating Table (Financial and Non-Financials**). Impact, on a 5 X 5 risk matrix, is broken into:

   - Insignificant
   - Minor
   - Moderate
   - Major
   - Severe/ Catastrophic

3. In determining and *level of likelihood* of each identified risk, management may consider the following questions in the event the risk crystallizes:

   a) What is the chance of the risk occurring in the next 12 months, 24 months and beyond 24 months?

b) In the past 1 to 5 years, has the risk occurred? If yes, what is the frequency per annum or within a specified time frame?
c) Are there any industry reports and/or benchmarks which would indicate that the risk identified may occur in the future?
d) Are there any reliable statistics or data or trends to predict the likelihood of the risk occurring in the future?

4. The responses received will be mapped against the risk parameter and appetite as shown in **Appendix 2 (Likelihood Rating Table)**. Likelihood, on a 5 X 5 risk matrix, is broken into:

- Rare
- Unlikely
- Possible
- Likely
- Almost Certain

5. Multiplying the risk's likelihood score with the risk's impact score generates the risk's overall risk rating score (Risk Rating = Likelihood Score X Impact Score). This value will be compared to other risks for prioritization purposes. Please refer below for a sample of a risk heat map/ matrix that visualizes the relationship between likelihood and impact:

Impact / Likelihood	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5

Rating	**Description**
Very High (VH)	Cause for concern. BRAC's/ Board's attention needed.
High (H)	Cause for concern. EXCO and Divisional/Departmental Heads' attention needed.
Medium (M)	On the watch list. Existing controls to be specified and monitored.
Low (L)	No major concern. Managed by routine procedures.

Step 6: Determine gross/inherent risk

1. Gross/ inherent risk refers to the significance of a risk in preventing the achievement of an organization's strategies and objectives, without considering the effectiveness of existing controls in place to manage the risk.

2. In this process, management can determine the overall gross/ inherent risk by tabulating/ plotting the risk consequence/ impact and likelihood (as determined in *Step 5*) into a risk heat map/ matrix. For example, Risk A was rated "High" at gross/ inherent level because of Management rating risk consequence/ impact as "Moderate", and risk likelihood as "Likely". *The gross/ inherent rating for Risk A* is shown in the risk heat map/ matrix below:

Consequence/ impact / ***Likelihood***	**Insignificant (1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Severe/Catastrophic (5)**
Almost certain (5)	M	H	H	VH	VH
Likely (4)	L	M	H **(Risk A)**	VH	VH
Possible (3)	L	M	M	H	H
Unlikely (2)	L	L	M	M	H
Rare (1)	L	L	L	L	M

3. The most significant risks in an organization are usually the ones located on the top right-hand area of the risk heat map/ matrix.

Step 7: Identify existing controls and its effectiveness

1. Upon determining the gross risk rating for each risk, management is to identify the existing controls to safeguard/ prevent those risks from transpiring. Controls are measures or actions in place that modifies or manages risk. It includes policy, procedure, process, practice, technology, techniques, methods or devices, which help ensure actions are taken to address risk. They are essential for proper stewardship and accountability of resources within an organization.

2. For an organization to achieve its strategies and objectives, controls should be embedded as an integral part of each business process. Strong controls reduce the risk of:

   a) Failure to meet organizational strategies and objectives
   b) Business breakdowns or unexpected results
   c) Excessive re-work to correct errors
   d) Erroneous management decision based on inaccurate, inadequate or misleading information
   e) Fraud, embezzlement and theft.

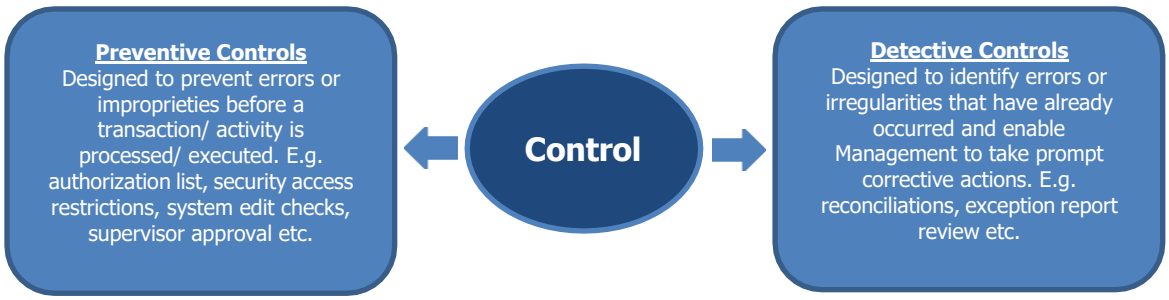
3. No one control provides all answers to risk management problems and thus cannot provide absolute assurance that it would eliminate the risk. In some situations, a combination of controls should be used whereas in others, one control may be sufficient in reducing risk.

4. An ideal control has the features of a carefully thought-out design, effective operation and are frequently updated whereby it generally has the following three (3) characteristics:

   a) It addresses the risk in question
   b) It is mandatory
   c) It is currently in operation

5. Control that strays from the ideal often disrupts the underlying business process and causes operational bottlenecks. As such, if an activity/ practice does not meet the abovementioned characteristics, it is not a control.

6. Control activities can be classified as preventive or detective as defined below:



7. With preventive and/ or detective controls in place, it would assist an organization to manage the risk against both consequence/ impact of the risk arising and the likelihood of the risk occurring.

8. The detective and preventive controls executed by management can be a combination of manual (i.e. performed by individuals), automated (i.e. incorporated into application systems) or IT-dependent manual (i.e. manually performed but require input based on the results of computer-produced information such as management's review of monthly variance report). Automated controls are considered more reliable due to their ability to prevent errors from being entered into the system and/ or detecting/ correcting errors in the system, whereas manual controls are more susceptible to human error.

9. Controls can also be considered soft or hard. Soft controls are those that provide notice of a requirement but do not immediately terminate a transaction for failing to meet the requirement (e.g. statutes, rules, policies and procedures), all of which tell people what should and should not be done. Soft controls are less effective if not paired up with hard controls. Hard controls are those that terminate a transaction/ activity for failing to meet a requirement (e.g. passwords, approvals, etc.). As such, by implementing just the soft control without its relevant hard control, it would not be effective in mitigating the risk. In other words, soft controls alone will not reduce the gross risk's consequences/ impact as well as the likelihood of the risk occurring.

10. Controls can be commonly categorized into the following types (this list is not an exhaustive list):

Types	Description
Documentation	Documentation preserves evidence to substantiate a decision, event, transaction of system. All documentation should be complete, accurate and recorded timely. Examples of areas where documents are important include documentation for critical decisions and significant events, transactions and policies and procedures.
Authorization and approval	Authorization is the power granted to an employee to perform a task and approval is the confirmation or sanction of employee's decision, events or transactions based on their individual review. This should be in line with the Group's Limits of Authority ("LOA").
Verification/ reconciliation	Verification/ reconciliation involves the comparison of an internally prepared document (e.g. purchase order) to an independent source (e.g. vendor invoice) to determine the completeness, accuracy, authenticity and/ or validity of transactions, events or information.
Segregation of duties	Segregation of duties is the division or separation of key duties and responsibilities among different employees to reduce the opportunity for any individual to be able to commit and conceal errors intentional or unintentional or perpetrate fraud in the normal course of their duties. This is to prevent any one individual from controlling and performing all key functions of transactions or events.
Access security	Limiting access to authorized individuals will assist in securing the access of resources and information to reduce the risk of unauthorized use or loss. Examples include system access, system configuration/ account mapping, limited key card access etc.
Supervision	Supervision is the ongoing oversight, management and guidance of an activity by designated employees to help ensure the results of the activity achieve the established objectives.
Reporting	Reporting is a means of conveying information on issues such as delays in project completion, payroll irregularities etc. whereby it helps promote accountability for actions and decisions.
Key performance indicators	Financial and non-financial quantitative measures that are collected, either continuously or periodically; and used by Management to evaluate the extent and progress towards meeting the organization's objective.

11. Once the existing controls have been identified, a self-assessment of its effectiveness is to be performed whereby management should consider how effective the existing controls are in managing the risk identified. As a guide, management may take the following questions into consideration to assist in determining the control and its effectiveness:

    a) Are roles, responsibilities and accountabilities defined and enforced?
    b) Is awareness communicated and followed?
    c) Are policies, procedures and guidelines defined and applied?
    d) Does existing controls and technology mitigate the key risks identified?
    e) Are existing auditing (self-audit and internal audit) and other independent assurance functions adequate to detect internal control weaknesses or lapses?

12. Subsequently, the following control effectiveness ratings can be used to assess the effectiveness of the existing controls:

Category	Description
Effective	Controls are strong and operating properly, providing a reasonable level of assurance that control objectives are being achieved.
Partially effective	Some control weaknesses/ inefficiencies have been identified. Although these are not considered to present serious risk exposure, improvements are required to provide a reasonable assurance that control objectives will be achieved.
Not effective	Controls do not meet an acceptable standard, as many weaknesses/ inefficiencies exist and do not provide reasonable assurance that control objectives will be achieved.

13. The effectiveness of the controls is assessed in terms of their control design strength and its overall ability to reduce the identified gross risk in terms of consequences/ impact and/ or likelihood of the risk occurring.

14. Once all the controls and its effectiveness are identified, it may become apparent that control gaps and redundancies exist upon determining the residual risk in Step 8. As controls are aimed at bringing the risk to fall within an organization's risk appetite, control gaps may occur when there is insufficient, or no controls taken to mitigate the risk.

<u>Step 8: Challenge the rating and determine residual risk</u>

1. Residual risk refers to the exposure presented by a risk in preventing the achievement of an organization's strategies and objectives *after considering the effectiveness of existing controls* in place to manage the risk. The difference between gross/ inherent risk and residual risk is the perceived/ estimated effectiveness of the controls in place.

2. The residual risk rating is a combination of the gross/ inherent rating in *Step 6* and considering control effectiveness in *Step 7.*

3. Management would need to understand the nature of existing controls identified to mitigate the risk, whether they address the risk cause(s) effectively, partially or not at all, and determine whether it would influence the risk consequence/ impact and/ or likelihood of the gross risk.

4. For example, Risk A was rated as "High" at gross/ inherent level (risk consequence/ impact rated as "Moderate" and risk likelihood rated as "Likely") under *Step 6*. It was determined by management that the risk arose due to uncontrollable external factors and as such, management has established one or more effective detective and soft controls to mitigate the risk. Upon considering these factors, management is of the view that these existing controls would influence the risk likelihood of the gross risk, i.e. from "Likely" to "Possible".

5. As such, the residual risk for Risk A is now rated as "Medium" (risk consequence/ impact rated as "Moderate" and risk likelihood rated as "Possible").

6. The movement of the gross/ inherent risk rating *to residual risk rating for Risk A* is shown in the risk heat map/ matrix below:

Consequence/ impact / ***Likelihood***	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe/Catastrophic (5)
Almost certain (5)	M	H	H	VH	VH
Likely (4)	L	M	H	VH	VH
Possible (3)	L	M	M **(Risk A)**	H	H
Unlikely (2)	L	L	M	M	H
Rare (1)	L	L	L	L	M

6.10 Risk evaluation

During this process, individual risk identified would be concluded based on the assessment of the control effectiveness associated with the risk identified. Subsequently, all active risks identified would be profiled i.e. on the risk heat map/ matrix, to enable risks to be prioritized on an individual and aggregate basis, to enable management to further treat the risk and perform monitoring as appropriate.

This process would ensure that all risks identified are within the risk parameter and appetite and appropriate action would need to be taken for risks that exceed the risk appetite.

Step 9: Determine the overall risk conclusion

Upon determining the residual risk in *Step 8*, a risk conclusion would be assigned to each residual risk to determine whether further risk treatment is required to be performed by management. A risk conclusion can be categorized and defined as follows:

Risk conclusion	**Description**	**Risk treatment plan required?**
Fully mitigated	Probability or consequences of threat are reduced to a reasonable level of assurance that risk will not materialize, if existing controls are working as intended.	No
Partially mitigated	There is the possibility of risk materializing. Improvements are required to ensure that the probability or consequences of threat are reduced to a reasonable level of assurance as existing controls are partially effective.	Yes (Proactive plan)
Not mitigated	Probability or consequences of threat are not reduced to a reasonable level of assurance whereby the risk may materialize as existing controls are not effective or not in placed.	Yes (Proactive plan)
Not rated	There is no possible control to reduce the probability of risk materializing as it is beyond the Group's capacity to control the risk.	Yes (Reactive plan)

Step 10: Develop risk profile

1. Risk profile shows a bird's eye view of the number of risks and potential effects of risks an organization faces. The risk profile also allows management to anticipate additional costs or disruption to operations as well as to obtain a high-level overview of the critical risk to assist in the risk prioritization (*Step 11*) to determine if risk treatment is required. Nonetheless, the risk profile also describes the willingness of an organization to take risks and how those risks will affect the strategies and objectives of the organization.

2. The risk profile should only include active risks. Inactive or emerging risks are to be included into the risk profile only when the risk becomes active. This is to allow management to focus its resources and efforts on active risks faced by the organization as it is more critical to the well-being of the organization.

3. A separate risk profile should be developed for the different risk levels to enable management to obtain a snapshot of the risks faced at the Group level, as well as divisional/departmental/project/vessel level.

Step 11: Prioritize risks

1. Risk prioritization is the process of identifying the most critical/ important risk at the Group level and at the Divisional/Departmental/individual project level whereby management's attention should be directed to focus on this risk.

2. To determine and prioritize the key risk, management should evaluate the risk by comparing the risk profiles developed in *Step 10* against the organization's risk parameter and appetite. This would assist management in determining whether the risk's magnitude is acceptable or tolerable.

3. Any risk that falls in the "RED" zone of the risk heat map/ matrix (as shown below) is defined as a risk requiring continuous and upmost attention, followed by 'ORANGE" zone, rather than focusing on risk falling in the "GREEN" zone.

4. In summary, the objective of risk management is not to eliminate all the residual risk but rather to ensure that they are maintained at an acceptable level in a cost-effective manner. There may be instances where management may decide to accept a "High" or "Very High" risk without developing any risk treatment plan to treat the risk – this should consider the degree of controls over the risk, the cost and reputational impact and the opportunities presented by accepting the risk.

6.11 Risk Treatment

The objective of a risk treatment plan is to achieve a targeted acceptable risk. Risk treatment could potentially reduce the consequence/ impact and/ or likelihood of a risk event. Risk treatment involves selecting one or more options to modify risks and implementing those options. Once implemented, risk treatment provides additional controls or modify the existing control.

Step 12: Formulate risk treatment plan

1. Having evaluated the risks in *Steps 9 to 11*, management should formulate a risk treatment plan which includes T.R.A.P – Termination (avoidance), Reduction, Acceptance and Pass-on (sharing). The following tasks shall be put in place to formulate and execute the risk treatment plan:

Task	Focus
Risk treatment plan	Determine the plan to be undertaken to manage the risk based on the risk treatment options as follows: ▪ ***Termination (avoidance):*** A decision to stop or not to start an initiative/ activity/ function as the potential risk impact outweighs the potential rewards (other risk responses are not viable) ▪ ***Reduction:*** Develop and implement action plans that will lessen the consequence/ impact and/ or the likelihood of the risk e.g. through organization procedures, improve processes, training, segregation of duties, internal monitoring system, expert advice, internal audit etc. ▪ ***Pass-on/ sharing:*** Transfer or share all or part of the risk with others e.g. insurance, joint ventures, partnership, outsourcing, hedging etc. ▪ ***Acceptance:*** A conscious business decision to 'accept' all or some risks as the potential gains outweigh the risk impact (other risk responses are not viable). In some cases, one risk treatment option may not mitigate the risk to an acceptable level and a combination of options may be appropriate.
Action cost	Ascertain the estimated cost for risk treatment. It should consider the cost/ benefit of the action. The most appropriate risk treatment involves balancing the costs and efforts of implementation against the benefits derived.
Expectations/ benefit	Ascertain the expected outcome to be generated from the planned action i.e. financial or non-financial. This expectation/ benefit shall then be used as a benchmark by management to check the action status upon completion of the action plan on the agreed completion date.
Risk owner	Identify a risk owner for leading or coordinating the action. Most individuals and teams will need to take some responsibility for risk management issues, but this will depend on their experience and time available.
Completion date	An action plan with a realistic completion date for each risk action should be determined and recorded. This may depend on the nature of the problem and action required; short-term actions can be deployed almost immediately; medium-term action normally requires a longer time of up to 6 months to be implemented; and long-term actions are those that will take more than 6 months to be implemented.
Treatment status	Progress of risk action plan must be updated to the RAC Department on a quarterly basis by the Divisional/Departmental Heads (or their delegated Risk Owners). The Head of RAC will report the implementation status to the CEO as and when appropriate.

6.12 Communication and Consultation

1. Communication and consultation with external and internal stakeholders is important throughout the risk management process to ensure the organization has a comprehensive picture of the risks it faces. It is a continual and interactive process that an organization conducts to provide, share or obtain information and engage in dialogue with stakeholders regarding the management of risk.

2. Internal communication should effectively convey the importance and relevance of effective enterprise risk management, the organization's objective, risk appetite and risk tolerance, a common risk language and roles and responsibilities of employees in effecting and supporting the components of enterprise risk management. It relates to management's ability to provide specific and direct communication that addresses behavioural expectations and the responsibilities of employees (e.g. clear LOA, policies and procedures, risk awareness training etc.). External communication involves conveying information to external parties such as charterer, broker, supplier, vendor, regulators etc. relevant to their needs so that they can understand readily the circumstances and risks the organization faces. Such communication should be meaningful, timely, pertinent, and conform to legal and regulatory requirements (e.g. upcoming developments, financial reports etc.).

3. As risk management takes place in a social context, information needs to be shared by people who are affected differently by a set of risks, who know different things about those risks, and who have different views about them. Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, considering confidential and employee integrity aspects.

6.13 Monitoring and Reporting

1. Monitoring and reporting are the process of periodically communicating risk related information throughout the organization and ultimately to the Board/ BRAC, whereby the RAC Department is responsible for coordinating all risk management related activities and reporting throughout the organization. Risk monitoring and reporting involves the following (among others):

    a) New risks are identified and considered as they arise
    b) Existing risks are monitored to identify any changes which may impact the Group
    c) Existing risk controls are still in place and working effectively (i.e. in both design and operation)
    d) Risk treatment plans are duly executed and are executed on a timely manner

2. The organization's monitoring and reporting process should encompass all aspects of the risk management process for the purpose of:

    a) Anticipating and responding in advance to risks that would otherwise impact the Group (i.e. via the formulation of risk treatment plan, considering lessons learn from past events/ near-misses, changes, trends, successes and failures)
    b) Reducing the ratification costs and other impacts associated with failing to respond to the risk in a timely manner
    c) Detecting activation of inactive risk and identification of emerging risks faced by the organization
    d) Creating a safer environment for the organization's stakeholders

3. All Divisional/Departmental Heads shall develop, maintain and update the overall risk profile (via snapshot of risk heat map/matrix) and respective Risk Registers and on a shared

online/digital platform, to be accessible by the RAC Department, CEO and the EXCO, for continuous monitoring. It shall specify:

a) Description of risk
b) Its root cause and impact
c) Gross risk rating (Before considering existing control(s))
d) An outline of the existing control(s)
e) Residual risk rating (After considering existing control(s))

A sample Risk Register is shown in **Appendix 3.**

4. As and when required, the Group's periodic reporting and monitoring process involves the following documentation:

Function	Reporting to	Reporting Frequency	Documentation
CEO	Board	Quarterly	▪ Group risk profile ▪ Risk treatment status and analysis for all high risks' areas
RAC Department	BARC	Quarterly	▪ Group risk profile ▪ Risk treatment status and analysis for all high risks' areas
Divisional/Departmental Heads/Risk Owners	RMC	Quarterly	▪ Divisional/Departmental Risk Profiles ▪ Risk registers including progress of risk treatment

APPENDICES

Appendix 1 – Risk Parameter and Appetite: Likelihood Rating Table

Rating	Likelihood	Description
5	Almost Certain	▪ Event is expected to occur in most circumstances, OR ▪ Will undoubtedly happen, possible frequency (e.g. annually/ frequently); OR ▪ Above 90% chance of occurring in the next 12 months; OR ▪ Imminent/ near miss
4	Likely	▪ Event will probably occur in some circumstances, OR ▪ Will probably happen but not a persistent issue, OR ▪ Below 90% but above 50% chance of occurring in the next 12 months; OR ▪ Has happened in the past
3	Possible	▪ Event might occur in certain circumstances, OR ▪ Might happen occasionally/ at some time, OR ▪ Below 50% but above 25% chance of occurring in the next 12 months; OR ▪ Has happened elsewhere
2	Unlikely	▪ Event could occur at some time, OR ▪ Below 25% but above 5% chance of occurring in the next 12 months; OR ▪ Not known in the activity
1	Rare	▪ Event may occur only in exceptional circumstance, OR ▪ Below 5% chance of occurring in the next 12 months, OR ▪ Is never likely to occur/ very unlikely this will ever happen

Appendix 2 – Risk Appetite and Parameter: Impact Rating Table (Financial)

Financial	**Impact and Score**				
	1	2	3	4	5
	Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Working Capital	Business as usual, able to manage working capital.	Unable to sustain working capital requirements for ≤ 1 quarter.	Unable to sustain working capital requirements for 1 – 2 quarters.	Unable to sustain working capital requirements for 3 – 4 quarters.	Unable to sustain working capital requirements for > 1 year.
PAT	Erosion of net profit amounting to < 3% PAT	Erosion of net profit amounting to 3% - 5% PAT	Erosion of net profit amounting to 5% - 8% PAT	Erosion of net profit amounting to 8% - 15% PAT	Erosion of net profit amounting to > 15% PAT
Asset Management	Asset damage amounting to < 1% total assets.	Asset damage amounting to 1% - 4% total assets.	Asset damage amounting to 4% - 7% total assets.	Asset damage amounting to 7% - 10% total assets.	Asset damage amounting to > 10% total assets.
Cashflow	Cash flow impact resolved without any financial assistance perspective.	Impact is resolved with internal arrangements within the Orkim Group.	Requires once-off funding from parent/holding company.	Requires periodical funding from parent/holding company.	Requires capital restructuring within the Orkim Group or may require external funding (financial institution).

(Con't) Appendix 2 – Risk Appetite and Parameter: Impact Rating Table (Non-Financial)

Non-financial	**Impact and Score**				
	1	2	3	4	5
	Insignificant	Minor	Moderate	Major	Severe
Reputation/ Media	Trust questioned – but recoverable speedily	Trust dented – recoverable with time and good public relations.	Trust diminished recoverable at considerable cost.	Trust significantly damaged – never fully recovered.	Trust completely lost – not recoverable.
Legal/ Regulatory/ Compliance/ Contractual obligation	Received a verbal or advice letter.	Received warning letter.	Fine/contractual penalty.	Heavy fine/ blacklisted.	Suspension of share, loss of license/ certification or closure of operations.
Health, Safety and Environment	▪ Emission rate <0.25% ▪ Spillage onboard <100 liters. ▪ Zero to slight injury – first aid case. ▪ Stable security environment	▪ Emission rate <0.5% ▪ Spillage onboard >100 liters and spill in the water <100 liters ▪ Minor injury requiring medical treatment. ▪ Security incidents noted, which require higher security levels for employees.	▪ Emission rate <1% ▪ Spillage onboard >100 liters and spill in the water >100 liters ▪ Major injury or health effects require hospitalization. ▪ Incidents/events are escalating which require constant security monitoring of further development.	▪ Emission rate >1% ▪ Spillage onboard >100 liters and spill in the water >1 cubic meter ▪ Single fatality or permanent total disability. ▪ Incidents/ events escalating to a point where business operations are disrupted.	▪ Emission rate > 2% ▪ Spillage onboard >100 liters and spill in the water >100 cubic meter. ▪ Multiple fatalities and permanent total disability. ▪ Incidents/ events have direct impact on the security of employees (injuries/fatalities)/ operation (corporate crimes).
Operations	▪ Supply chain disruption < 6 hours. ▪ Limited business disruption < 6 hours. No intervention required from management. Impact absorbed through normal activity.	▪ Supply chain disruption > 1 day ▪ Minimal business disruption up to 1 day. Requires middle management intervention (Managers/ Senior Managers)	▪ Supply chain disruption > 1 week. ▪ Significant business disruption up to 1 week. Requires Management Committee's intervention (Senior Manager/ Head of Department).	▪ Supply chain disruption > 1 month. ▪ Major business disruption up to 1 month. Requires intervention from EXCO/Operating Committee.	▪ Supply chain disruption > 3 months. ▪ Severe business disruption > 1 month. Requires intervention from the Board of Directors.

(Con't) Appendix 2 – Risk Appetite and Parameter: Impact Rating Table (Non-Financial)

Non-financial	Impact and Score				
	1	2	3	4	5
	Insignificant	Minor	Moderate	Major	Severe
Corruption	Low-level policy/ procedural violations with no financial or reputational damage. Tolerable within predefined boundaries, with swift corrective actions.	Isolated incidents of unethical misconduct that result in internal disciplinary action. Lessons learned include strengthening controls and proactive monitoring required.	Systemic ethical weaknesses lead to recurring compliance failures and financial losses.	Ethical misconduct cases involving senior leadership with regulatory scrutiny, impacting shareholder's confidence.	Large-scale fraud, legal action, regulatory enforcement, loss of public trust and severe reputational damage.
Stakeholders – customers or vendors	Minimal service disruptions, minor complaints or slight deviations in supply chain performance, provided corrective measures are swiftly implemented to prevent recurrence.	Isolated service dissatisfaction, occasional delays from vendors or minor contract compliance issues that require operational adjustments, requiring proactive supplier engagement and customer relationship management.	Repeated service quality concerns, medium-scale supply chain disruptions affecting cost efficiency or reputational risks arising from vendor compliance failures.	Loss of key customers due to dissatisfaction, critical vendor failures leading to operational delays that affect business credibility.	Large-scale customer attrition, supplier bankruptcy or legal violations, severe regulatory breaches or irreversible reputational damage necessitating crisis management protocols.
Stakeholders - employees	Minor workplace dissatisfaction, isolated complaints or temporary productivity dips, addressed through regular engagement and internal communication.	Low staff morale or minor disputes that affect team dynamics. Proactive measures required to ensure retention and maintain employee satisfaction.	Recurring workforce grievances, increasing turnover rates or moderate operational inefficiencies due to disengaged employees, requiring mitigation strategies to enhance leadership engagement.	Significant employee dissatisfaction leads to decreased performance, loss of critical talent or potential labour disputes, requires intervention through leadership alignment.	Large-scale workforce unrest, regulatory scrutiny due to labour law violations and reputational crises resulting from employee-related issues.

Appendix 3 – Sample of Risk Registers for Guidance – Finance Department

Risk ID	Risk Objective	Risk Category	Risk Owner	Risk Name and Description	Root Cause	Gross Risk			Residual Risk				Risk Mitigation Strategies
						Likelihood	Impact	Risk Level	Likelihood	Impact	Risk Level	Treatment Type	
	Strengthen Financial Sustainability: i) To ensure cash available for sukuk repayment as per maturity date ii)Dividend Payout to Shareholder	Operational		**Name:**Online Payment Risk **Description:**The company exposed to online payment risk when the method of payment was changed from the bank cheque to the internet banking. The Company was exposed to risk arising from scammers.	1.Cyber Security Weakness 2.Employee Negligence	4	5	20	1	5	5	Reduce	
	Strengthen Financial Sustainability: ii)To ensure on a timely basis the expected income	Financial		**Name:**Poor Debt Collection **Description:**An accumulation of bad debt can soon give detrimental effects to cash flow issues by causing a slowdown in income which limits the amount of cash available for operation and expansion of business	1.Documentations on billing and aging not properly monitor 2.Inefficient customer screening method	4	5	20	2	1	2	Reduce	
	Internal Reporting:Prepare monthly estimate	Financial		**Name:**Cost over budgeted **Description:** The company exposed to overrun budget due to actual cost exceed the estimation.	1.Uncertainty of foreign exchange 2.Changes in government policies & regulation 3.Disruption in geopolitical condition 4.Poor budget planning	4	3	12	1	1	1	Reduce	
	Improve internal efficiency:	Financial		**Name:**Inability to meet liability commitment **Description:**Inability to meet it's financial obligation in term of l.e; 1.Shareholder dividend commitment 2.Loan & borrowings	1.Excessive borrowings. 2.Cash flow constraint 3.Vulnerable to fluctuation in interest rate ,high finance cost	4	3	12	2	1	2	Reduce	
	Strengthen Financial Sustainability	Financial		**Name:** Inaccurate Financial Reporting **Description:**The risk of inaccurate financial reporting can occurs due to intentional or unintentional error	1.Data accounting error 2.Inadequately trained staff/incompetent staff 3.Inaccurate review process 4.Flaws in the system or poorly integrated financial system 5.Difficulty in understanding the accounting system 6.Fraud	4	3	12	2	1	2	avoid	