

	Document Type: POLICY AND FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Revision:	Rev. 1
		Date Published:	23 April 2026

MMC ENGINEERING SDN BHD
(125132-T)

**MMC ENGINEERING & CONSTRUCTION
SDN BHD**
(215783-X)

**ENTERPRISE RISK MANAGEMENT
POLICY AND FRAMEWORK**



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 2 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026


TABLE OF CONTENTS

Amendment Page.....	3
1.0 Introduction	4
2.0 Policy Statement	4
3.0 Objectives	5
4.0 Enterprise Risk Management Framework.....	5
5.0 Reporting Requirement	7
6.0 Enterprise Risk Management Process.....	7
7.0 Roles And Responsibility.....	8
8.0 Confidentiality.....	9
9.0 Document Changes.....	9
Appendix 1: Enterprise Risk Management Process	10
Appendix 2: Risk Coordinator Roles and Responsibilities	20
Appendix 3: Risk Owner Roles and Responsibilities	21



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Page: Page 3 of 21
			Revision: Rev. 1
			Date Published: 23 April 2026

AMENDMENT PAGE

Revision No.	Date	Description Of Change	Reason For Change	Signature / Initial
Initial release	23 April 2015	Initial release	Nil	
1	7 April 2026	<p>Introduction, Page 4</p> <p>Administrative changes in Appendix 1, Appendix 2 and Appendix 3.</p> <p>Inclusion of new ISO 31000 version i.e. from version 2008 to version 2018.</p>	<ul style="list-style-type: none"> - Change of Company Name from MMC Engineering Services Sdn Bhd (MMCES) to MMC Engineering Sdn Bhd and MMC Engineering & Construction Sdn Bhd (MMCE & MMCEC) - To represent the current process - Remove Terms of Reference (TOR), with ERM to be updated through Enterprise Risk Management System (Tricor Radar) submission every quarter. <p style="text-align: center;">and;</p> <p>Project Risk Assessment to be updated through Project Team by Monthly/ Quarterly basis, refer Project Risk Management Plan.</p> <ul style="list-style-type: none"> - Change in ISO 31000 version. Adopted from MMC ERM Policy & Framework Rev 3.0. 	



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 4 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026

1.0 INTRODUCTION

Risk management is a part of MMC Engineering Sdn Bhd and MMC Engineering & Construction Sdn Bhd ("MMCE & MMCEC" or "the Company") strategy to promote accountability through good governance and robust business practices to support our 4 strategic objectives:

- i. Maximise Shareholder Value
- ii. Service Excellence to Stakeholders
- iii. Lead in Value Innovation
- iv. Be the Preferred Employer

The Enterprise Risk Management Policy and Framework ("Framework") sets out the process for managing risks across the Company. This Framework outlines how the organization ensures risks are managed effectively and efficiently. It illustrates how risk management is embedded in our organizational systems to ensure that it is integrated at all levels and work contexts. It describes the key principles, elements and processes to guide staff in effectively managing risks, making it part of our day-to-day decision-making and business practices.

MMCE & MMCEC applies risk management across the entire organisation. Implementation of the Framework strengthens management practices, decision making and resource allocation process, while at the same time protects stakeholders' interests and maintains trust and confidence.

This Framework shall be guided largely by the Enterprise Risk Management Policy and Framework, Third Edition 2024 adopted by MMC Corporation Berhad ("MMCB"). The Company Framework shall be approved by MMCE & MMCEC's Board of Director

2.0 POLICY STATEMENT

MMCE & MMCEC is committed to embed risk management principles and practices into its organisational culture, governance, planning, reporting, performance review, business transformation and improvement processes. MMCE & MMCEC will establish and communicate its risk appetite to guide staff in their actions relating to the organisation's risk acceptance level. To position the Company as a risk-aware, responsive and resilient organisation, our risk management approach is directed through:

- i. Keeping abreast with external and internal developments and risks which can have an effect on the organization.
- ii. Effective identification and management of risks at all levels in the organization.
- iii. Compliance with relevant legislation, policies and procedures.
- iv. Alignment with standards and best practices to soundly support decision making and continuous improvement of our risk management practices.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 5 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026

Effective risk management practice is modelled by:

- i. Leadership demonstrated by the Board of Directors, Chief Executive Officer and Management Teams.
- ii. Staff in all work contexts through their identification, analysis, evaluation, treatment, monitoring and review of risks that may impact on achieving our organisational purpose and objectives.

3.0 OBJECTIVES

The objectives of the Framework are as follows: -

- i. Provide a policy and organizational structure for the management of risks within the Company.
- ii. Define risk management roles and responsibilities within the Company and outlining procedures to mitigate risks.
- iii. Ensure consistent and acceptable risk management practices throughout the Company.
- iv. Define the reporting framework to ensure clear communication on all risk management activities and reporting.
- v. Accommodate the changing risk management needs of the Company while maintaining control of overall risks.
- vi. Detail the approved methodology for risk assessment.
- vii. Provide centralized consolidation of risk management data and reporting.

4.0 ENTERPRISE RISK MANAGEMENT FRAMEWORK


Enterprise Risk Management ("ERM") is a process adopted by the Board, Management and all personnel. It is applied in a strategy setting across the organisation (including for projects and by subsidiaries, if applicable) to assist in identifying risks and manage it effectively. This is to provide reasonable assurance on the achievement of business objectives.

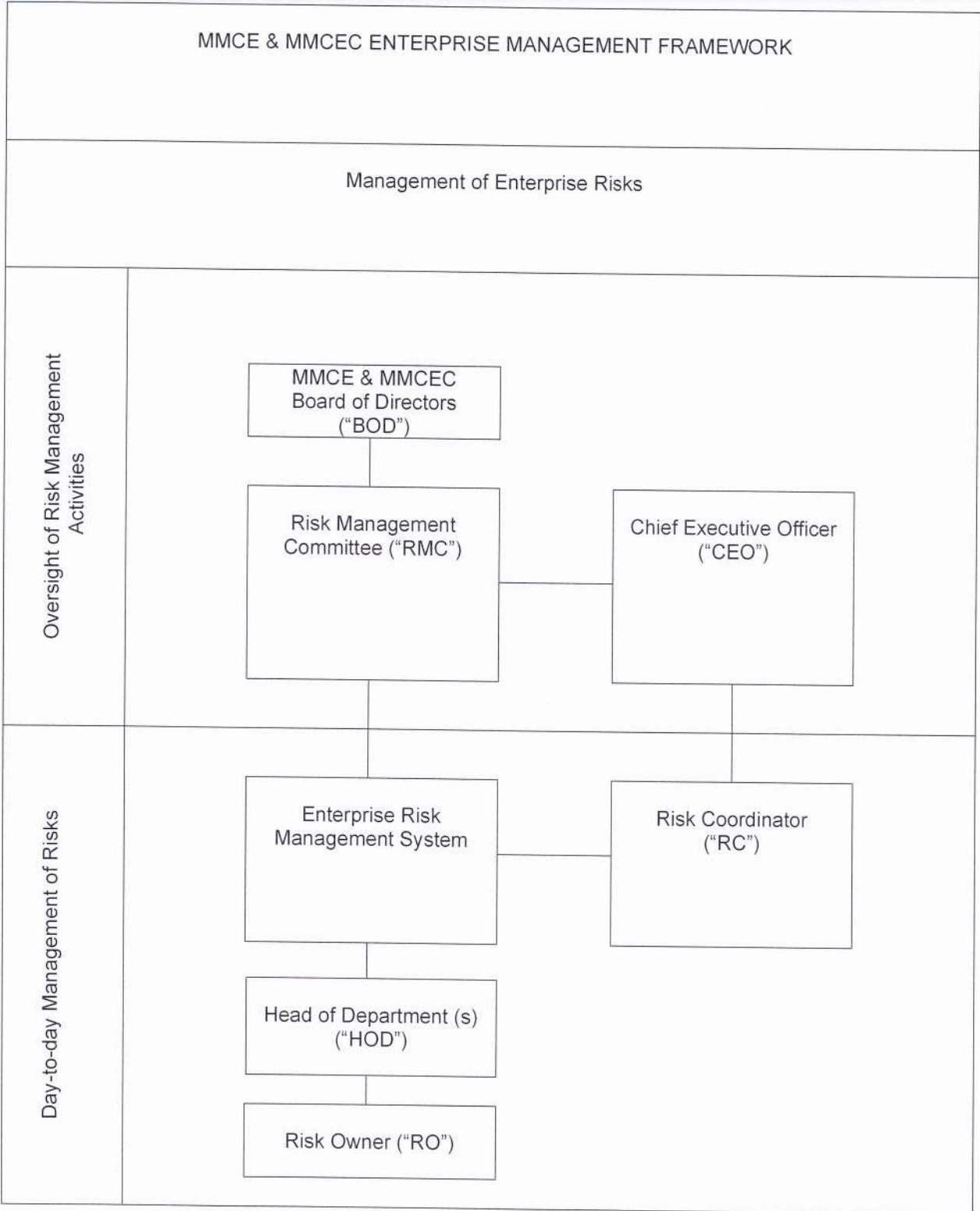
The ERM Framework helps to ensure that risks are managed across the Company in a holistic manner, is integrated into our culture, business practices and business plans, is inclusive of all levels of staff and is applied in a consistent manner.

ERM supports the needs of the Company. The most important element of this structure is the clear definition and communication of the roles, responsibilities and accountabilities for managing risks within the organization.

An overall overview of the Framework of MMCE & MMCEC is provided in the diagram below. The diagram illustrates the key elements necessary for managing risk and the integration of these elements at all levels and in all work contexts.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 6 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Page: Page 7 of 21
			Revision: Rev. 1
			Date Published: 23 April 2026

5.0 REPORTING REQUIREMENT

The establishment and implementation of the ERM framework requires the Company to submit quarterly risk management reports or as and when required based on the emergence of new risks following the Group's risk management organization structure via an enterprise risk management system.

6.0 ENTERPRISE RISK MANAGEMENT PROCESS

MMCE & MMCEC adopts ISO 31000:2018 in its risk management process. Figure 1 below illustrates the steps of the risk management process. The detailed process is set out in *Appendix 1*.

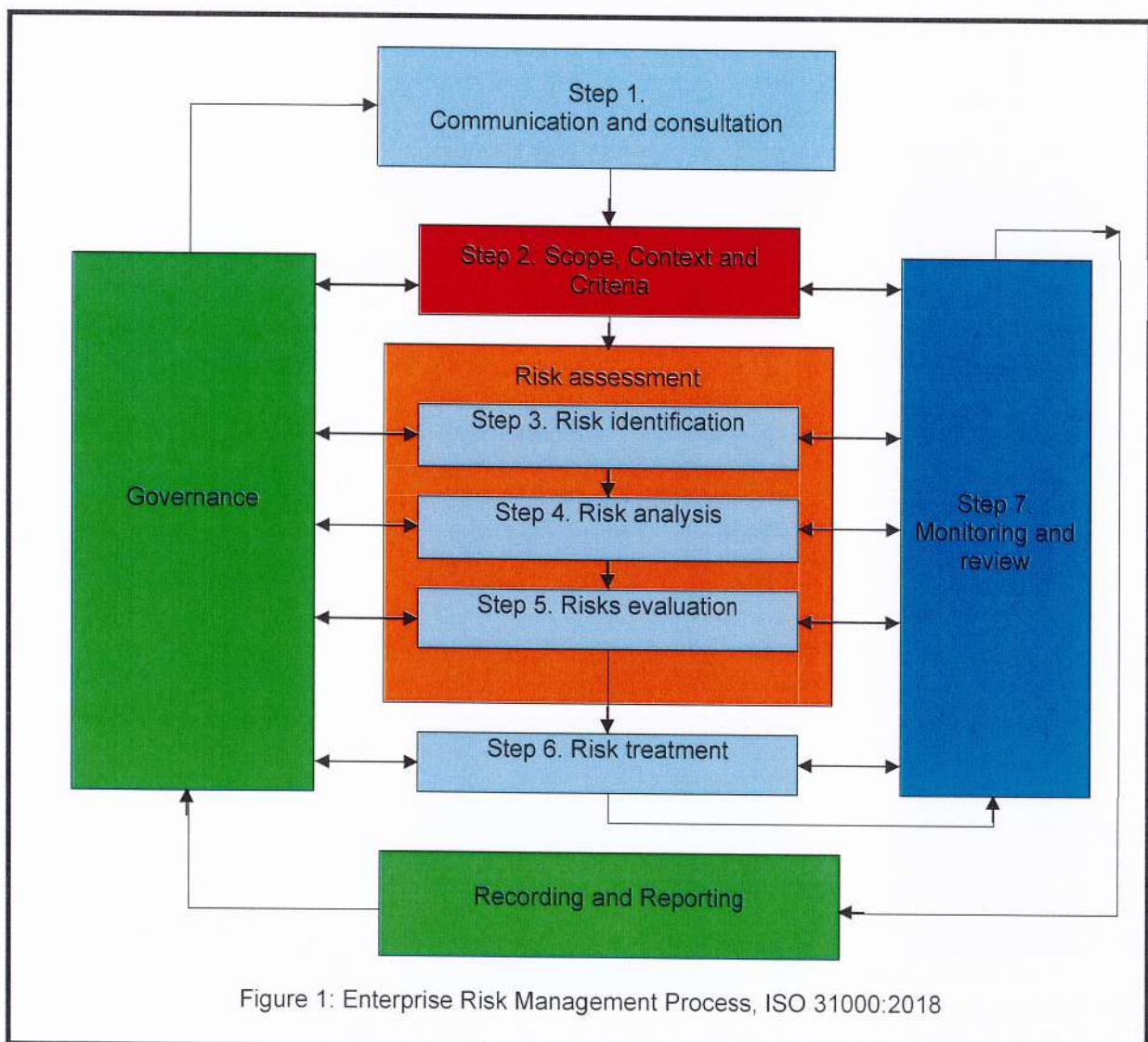



Figure 1: Enterprise Risk Management Process, ISO 31000:2018



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 8 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026

7.0 ROLES AND RESPONSIBILITIES

7.1 Board of Directors

MMCE & MMCEC's Board of Directors ("BOD") is ultimately responsible for all elements of risk management and internal control of the Company. This is consistent with the principal responsibilities of the Board of Directors as set out under the Malaysian Code of Corporate Governance.

The BOD shall:

- i. Satisfy itself that significant risks faced by MMCE & MMCEC are being managed appropriately and that the system of risk management within the Company is robust enough to respond to changes in the business environment.
- ii. Ensure that an appropriate organization and reporting structure as well as system are established to support the delivery and communication of this Framework on an on-going basis.
- iii. Adequately discuss and provide challenge on issues of risk and opportunity, their treatment and the overall risk appetite and risk portfolio of MMCE & MMCEC.

The BOD, who is responsible for the system of risk management and internal control of MMCE & MMCEC, has delegated the above responsibility to the Risk Management Committee ("RMC").

7.2 Risk Management Committee ("RMC")

RMC is responsible for assisting the BOD to oversee the establishment and implementation of an enterprise risk management system. The RMC is also responsible for reviewing the effectiveness of the system annually.

7.3 Risk Coordinator ("RC")


RC will be responsible for risk reporting, risk monitoring, risk advisory and risk communication within MMCE & MMCEC.

The RC roles and responsibilities are to be incorporated into the Risk Coordinator job descriptions.

The RC plays an important role in ensuring the successful establishment and implementation of the ERM framework throughout the Company.

The detailed roles and responsibilities of the RC are as per **Appendix 2**.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 9 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026

7.4 Risk Owner ("RO")

RO is a named individual accountable for all aspects of the risk including identification, assessment, evaluation, monitoring and reporting for the area under their purview. He/she is the best person to take appropriate decisions and adequate control to manage the risk in question.

The detailed roles and responsibilities of the RO are attached in **Appendix 3**.

7.5 Management and Head of Department

The Management and Head of Department ("HOD") has a frontline responsibility for identifying and evaluating risks within their area of responsibility, implementing agreed actions to manage risk and for reporting any activity or circumstance that may give rise to new or changed risks.

Management and the HOD shall ensure that appropriate controls are in place to manage identified risks including the formulation of preventive and contingency plans where necessary by performing monthly compliance and assessment in the ERM risk register.

7.6 Employees

All employees have a general duty of care and are responsible to comply with the Framework. It is the duty of all MMCE & MMCEC employees to be conscious of the risks related to their actions and decisions.

8.0 CONFIDENTIALITY

The information contained within any document dealing with MMCE & MMCEC's business risks is to be treated as highly CONFIDENTIAL and should not be released to any outside parties without the prior consent of the BOD.

9.0 DOCUMENT CHANGES

This document is authorized by the BOD. It is a controlled document and is subject to update and if copied, must be marked "Uncontrolled Copy".

Changes are only be authorized by the BOD. Any change to this Framework will result in a change to the revision status and complete reissuance of the Framework.

Records of all changes made to the Framework shall be maintained by the RC



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 10 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026

APPENDIX 1

ENTERPRISE RISK MANAGEMENT PROCESS

Step 1: Communication and Consultation

- Communication and consultation with internal and external stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage.
- These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

Step 2: Establishing the Context

- By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process.
 - i. Establishing the external context
 - a. The external context is the external environment in which the organization seeks to achieve its objectives.
 - b. Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.
 - c. The external context can include but is not limited to:
 - The social and cultural, political, legal, regulatory, financial, technological and economic.
 - Competitive environment. whether international, national, regional or local.
 - Key drivers and trends having impact on the objectives of the organization.
 - Relationships with, perceptions and values of external stakeholders.
 - ii. Establishing the internal context
 - a. The internal context is the internal environment in which the organization seeks to achieve its objectives.
 - b. The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risks.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 11 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026

c. It is necessary to understand the internal context. This can include, but is not limited to:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- Capabilities, understood in terms of resources and knowledge (e.g. Capital, time, people, processes, systems and technologies);
- The relationships with and perceptions and values of internal stakeholders;
- The organization's culture;
- Information systems, information flows and decision-making processes (both formal and informal);
- Standards, guidelines and models adopted by the organization; and
- Form and extent of contractual relationships.

iii. Establishing the context of the risk management process

- a. The objectives, strategies scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of risks should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.
- b. The context of the risk management process will vary according to the needs of an organization. It can involve, but is not limited to:
- Defining the goals and objectives of the risk management activities;
 - Defining responsibilities for and within the risk management process;
 - Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions
 - Defining the activity, process, function, project, product, service or asset in terms of time and location;
 - Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization;
 - Defining the risk assessment methodologies;
 - Defining the way performance and effectiveness is evaluated in the management of risk;
 - Identifying and specifying the decisions that have to be made; and
 - Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.
 - Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the organization and to the risks affecting the achievement of its objectives.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 12 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026

iv. Defining risk criteria

- a. The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy, be defined at the beginning of any risk management process and be continually reviewed.
- b. When defining risk criteria, factors to be considered should include the following:
 - The nature and types of causes and consequences that can occur and how they will be measured;
 - How likelihood will be defined;
 - The timeframe(s) of the likelihood and/or consequence(s);
 - How the level of risk is to be determined;
 - The views of stakeholders;
 - The level at which risk becomes acceptable or tolerable; and
 - Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

Risk Assessment

Risk Assessment is the overall process of risk identification, risk analysis and risk evaluation.

Step 3: Risk Identification

- Risk identification is a line management's responsibility. All risks identified will be evaluated and documented, together with the controls, action plans and a Risk Owner who is accountable for the risks.
- For each risk, accountability is assigned to the person best able to take appropriate decisions to manage the risk in question.
- A Risk Owner is a named individual accountable for all aspects of the risk including assessment, evaluation, monitoring and reporting.
- The responsibility of the adequacy of control of each risk rests with the assigned risk owner.
- Risk Owners may delegate tasks of managing the risks to others. However, the responsibility over the risks still remains with the Risk Owner. The delegated task owner would then report the progress back to the Risk Owner.
- The Risk Register records details of all the risks identified, their grading in terms of likelihood of occurring and seriousness of impact to MMCE & MMCEC's, existing controls on identified risk, plans for mitigating the risk, the costs and responsibilities of the prescribed mitigation strategies and subsequent results.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner: QUALITY & RISK DEPARTMENT (MMCE & MMCEC)	Page:	Page 13 of 21
		Revision:	Rev. 1
		Date Published:	23 April 2026

- The sample risk registers to be used consist of the following:

Part 1: Risk Identification & Measurement

- Risk Tag
- Risk Title
- Risk Description – A clear description of the risk
- Risk Category
- Risk Owner (a person responsible to manage the risk)
- Cause – Internal and/or external causes
- Consequences – the impact of the risk to the department, company and/or group.

Part 2: Risk Rating (Likelihood + Impact)

- Gross Risk Rating – Risk ratings (likelihood and impact) BEFORE the consideration of current control effectiveness.
- Nett Risk Rating – Risk ratings (likelihood and impact) AFTER the consideration of current control effectiveness.
- Target Risk Rating – Risk ratings (likelihood and impact) AFTER the completion of management action plans.

Part 3: Risk Treatment – include the selection, design and implementation of risk treatment options.

- Control – list of controls in placed to mitigate the risk
- Control name and description
- Control Owner (a person responsible to manage the control)
- Assessment on Control Effectiveness – Very good/Good/Satisfactory/Some Weakness/Weak

Part 4: Management Action – List of additional control to further mitigate the risk.

If after applying the control(s) the risk status is acceptable then the risk should be tolerated; there is nothing more to do. But if the status remains unacceptable (bearing in mind our risk appetite) then further mitigating action is required. The steps are as follows:

- The Start and Due date of the management action
- Name and description of the management action
- Management Action Owner (a person responsible to manage the management action)
- Status – Status of management action i.e. Completed/ Due/ Postpone/ In Progress as Planned/ Not yet started
- Remark – to track the progress of management action until its completion



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001	
	Document Owner:		Page:	
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision:	Page 14 of 21
			Date Published:	Rev. 1
			23 April 2026	

- Risk Categories

Risk categories can be defined as the classification of risks as per the business activities of the organization and provides a structured overview of the underlying and potential risks faced by the organization. The organization list of risk categories (non-exhaustive) as per below table: -

No.	Risk Category	Description
1	Financial Risk	Exposure related to loss of monetary resources or incurring unacceptable liabilities.
2	Business & Strategic Risk	<ul style="list-style-type: none"> Exposure to uncertainty arising from long-term or short-term, policy decisions based on current strategy of operating unit. Exposure to uncertainty due to competition and/or fiscal policy changes. Risks that are external to the operating unit and beyond the control of the organization.
3	Operational Risk	Exposure to uncertainty arising from daily tactical business activities related to Business Processes & Technology.
4	Reputation Risk	Exposure to uncertainty arising from organization brand or image.
5	Information Risk	Exposure to uncertainty arising from loss or inaccuracy of data, IT systems or reported information.
6	Organization Risk	<ul style="list-style-type: none"> Risks arising from poor communication systems property/casualty insurance. Risk associated with organizational structure, employees (skills, competency, etc.) and management.
7	Regulatory Risk	Exposure to uncertainty arising from inadequacy in compliance to required mandatory or established regulations and policies.
8	Fraud Risk	Exposure to uncertainty arising from dishonest act with intend to cheat in a corporation whereby certain parties may unlawfully benefit from the act/deal.
9	Market Risk	Exposure to uncertainty arising from economic factors such as FOREX, commodity prices etc.
10	Cyber Security Risk	The potential exposure or loss resulting from a cyberattack or data breach within an organization.
11	Bribery and Corruption Risk	The potential for individuals or organizations to engage in unethical or illegal activities, such as offering or accepting bribes, in order to gain an unfair advantage or manipulate situation.
12	Project Risk	A project risk is an uncertain event or condition that may or may not occur during a project.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 15 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026

Step 4: Risk Analysis

- Risk analysis allows an entity to consider the extent to which the potential events might have an impact on the achievement of the company's objectives.
- The overall Risk Score is considering the **SUM** of Risk **LIKELIHOOD** and **CONSEQUENCES** rating.
- The Risk Likelihood measurement below is a default measurement based on the expected frequency of risk occurring every quarter. This measurement may be adjusted based on the MMCE & MMCEC's performance.

Scales	Probability	Description
Almost Certain	> 75%	Almost certain to occur
Likely	51% - 75%	More likely to occur than not
Possible	26% - 50%	Fairly likely to occur
Unlikely	6% - 25%	Unlikely to occur
Rare	0% - 5%	Extremely unlikely

- **Risk Matrix** - A grading of each risk according to a risk assessment matrix is tabulated below. A table is used to calculate the **CONSEQUENCES + LIKELIHOOD** of risk occurrence. Scoring is then given to provide an indication of the magnitude of the risk to MMCE & MMCEC's.

CONSEQUENCES \ LIKELIHOOD	CONSEQUENCES				
	Insignificant	Minor	Moderate	Major	Severe
Almost Certain	6	7	8	9	10
Likely	5	6	7	8	9
Possible	4	5	6	7	8
Unlikely	3	4	5	6	7
Rare	2	3	4	5	6

Risk Ratings (Risk Score)	EXTREME (8-10)	HIGH (6-7)	MODERATE (4-5)	LOW (2-3)
---------------------------	-----------------------	-------------------	-----------------------	------------------

Risk Matrix Table



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001	
	Document Owner:		Page:	
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision:	Page 16 of 21
			Date Published:	Rev. 1
			23 April 2026	

- **Risk Parameters** - The parameter on setting the impact is tabulated below.


FACTOR	CONSEQUENCES (FINANCIAL & NON-FINANCIAL)				
	Insignificant	Minor	Moderate	Major	Catastrophic
1. Revenue against Budget for the FY	< 1 %	< 3 %	< 5 %	< 10 %	> 10 %
2. Impact on PBT against budget for the FY	< 1 %	< 3 %	< 5 %	< 10 %	> 10 %
3. Investment income budget for the FY (Dividend at MMCE & MMCEC level)	< 1 %	< 3 %	< 5 %	< 10 %	> 10 %
4. Shortfall of new businesses / projects against budget for the FY	< 10 %	< 20 %	< 30 %	< 40 %	> 40 %
5. Impairment of Asset / Investment against value / cost	< 1 %	< 3 %	< 5 %	< 10 %	> 10 %
6. Funds Availability	Sustainable more than 4 months	Sustainable less than 4 months	Sustainable less than 3 months	Sustainable less than 2 months	Sustainable less than 1 month
7. Project Management	Project delay <1% of budgeted timeline. or Cost Overrun of <1% of contract value (by project type).	Project delay <3% of budgeted timeline. or Cost Overrun of <3% of contract value (by project type).	Project delay <5% of budgeted timeline. or Cost Overrun of <5% of contract value (by project type).	Project delay < 10% of budgeted timeline. or Cost Overrun of <10% of contract value (by project type).	Project delay > 10% of budgeted timeline. or Cost Overrun of >10% of contract value (by project type).
8. Occupational, Health & Safety	First Aid only required	Minor medical treatment with or without potential for lost time.	Significant injury involving medical treatment or hospitalization and lost time.	Individual fatality or serious long term injury.	Multiple fatalities or extensive long term injury.
9. Image & Reputation	Isolated, internal or minimal adverse attention or complaint.	Heightened local community concern or criticism.	Significant public criticism with or without media attention.	Serious public or media outcry; broad media attention.	Extensive public outcry; potential national media attention.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 17 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026

10. Environmental & Natural Hazards	Minimal physical or environmental impact; isolated hazards only; dealt with through normal operations.	Minor physical or environmental impact; hazards immediately controlled with local resources.	Significant physical or environmental impact; hazards contained with assistance of external resources.	Major physical or environmental impact; hazard extending off-site; external services required to manage.	Extensive physical or environmental impact extending off-site; managed by external services; long term remediation required.
11. Regulatory & Governance	Isolated non-compliance or breach; minimal failure of internal controls managed by normal operations.	Contained non-compliance or breach with short term significance; some impact on normal operations.	Serious breach involving statutory authority or investigation; significant failure of internal controls; adverse publicity at local level.	Major breach with formal inquiry; critical failure of internal controls; widespread adverse publicity.	Extensive breach involving multiple individuals; potential litigation; viability of organization threatened.
12. Contractual & Legal	Isolated non-compliance or breach; negligible financial and non-financial impact. (Non-financial impact can include loss of reputation, goodwill, customer confidence, opportunities, loss of employee morale etc.)	Contained non-compliance or breach with short term significance and minor financial and non-financial impact.	Serious breach and non-compliance including prosecution by relevant statutory authority/authorities with some adverse financial and non-financial impact.	Major breach and non-compliance leading to major fines/penalty and legal claims; with long term significance and major adverse financial and non-financial impact.	Massive fined/penalty and legal claims with possible threat to viability of project or company leading to massive adverse financial and non-financial impact.
13. Human Resource	<10% of staff turnover excluding key management	<15% of staff turnover excluding key management	<20% of staff turnover including key management	<25% of staff turnover including key management	>25% of staff turnover including key management
	Employees Satisfaction Index > 80%	Employees Satisfaction Index < 80%	Employees Satisfaction Index < 72%	Employees Satisfaction Index < 65%	Employees Satisfaction Index < 50%



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 18 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026

Step 5: Risk Evaluation

- The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.
- It is the responsibility of the relevant operational and functional heads to implement the mitigation strategies identified in the Risk Register developed during the Risk Identification process.
- Where current controls are deemed ineffective, appropriate actions plans will be developed by the management to mitigate the risks. Allocation of accountabilities and action dates for the implementation of the action plans need to be established. Risk mitigation strategies involves identifying the range or options for treating risks, assessing those options, preparing action plans and implementing those plans.
- The Action Plans must follow the **“SMART”** principles:

Specific	Action Plans must be detailed and exact.
Measurable	Action Plans must be measurable in nature i.e. financial impact,
Achievable	Action Plans must have a targeted objective that is achievable
Realistic	Action Plans must be realistic where actual results can be produced.
Time-Based	Action Plans must have time-line for execution and targeted achievement results.

Step 6: Risk Treatment

- Risk Treatment is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include terminate, reduce, accept, pass and spread the risk (TRAPS).
- The treatment plan is how to plan to respond to potential risks. It outlines how risks will be managed whether they are low, high, or acceptable risks. The controls set in the risk management plan will assign team members or stakeholders the task or how they will respond to risk.

Terminate	By deciding not to process or avoid the activity likely to generate risks
Reduce	Introducing controls or action plans to reduce the significance of the risks
Accept	Using the abilities of the Group to accept the risks in order to build a competitive edge over other competitors.
Pass	By transferring the consequences of risks to third parties e.g. insurance, hedging, etc.
Spread	By sharing the occurrence of risks with third parties e.g. joint ventures, outsourcing, etc.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 19 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026

Step 7: Monitoring and Review

- The objectives of monitoring and reviewing the risk management process is to provide reasonable assurance that risks are being managed effectively. It is also to ensure that risk profiles drawn up reflect changing business conditions and exposures. Formal reporting has been instituted at the departmental, corporate and Board levels (including the Operating Companies Board) and contain the significant risks identified by the business during the period.
- The objectives are achieved through the deployment and implementation of the following activities:
 - a. Digital confirmation (Corporate Digital Assurance) – Risk Owner, Control Owner and Management Action Owner shall review and provide an assurance on their respective risk, control and management action on a quarterly basis.
 - b. The Head of the Company, Head of Division or Head of Department (Risk Scorecard Owner) shall then if deem fit to approve the risk scorecard under his/her purview.
 - c. Internal Audit Reviews, which are undertaken according to Annual Group Internal Audit Plan, provides independent assurance on the adequacy, existence and effectiveness of the governance, risk management and control processes.
- The Company should continually improve their risk management process including continually monitoring and adapting the framework to address external and internal changes; taking actions to improve the value of risk management; and improving the suitability, adequacy and effectiveness of the risk management framework.

Step 8: Recording and Reporting

- The Company risk profiles are recorded through an enterprise risk management system, namely the Tricor-Radar Enterprise Risk Management System, an online monitoring and database system for risk management. The system enables online real-time updates and monitoring of risk management record profiles for the Company.
- Regular risk reporting is essential for information management and business planning. Formal reporting has been instituted at various levels of the organization (including the Subsidiaries' Board) by MMCEB to highlight the significant risks identified by the business during the previous period and business planning cycles.
- On a quarterly basis, the CEO of MMCE & MMCEC will assess and update the relevant risk information via the Enterprise Risk Management System.
- For the purpose of the quarterly risk management reporting to the MMCEB's RMC, MMCE & MMCEC's RMC should only extract from the system the risks that are rated as "high" and above (as per MMCE & MMCEC's established risk score).
- MMCE & MMCEC is also required to table its risks that are rated as "high" and above to its BOD on a quarterly basis.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 20 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026


APPENDIX 2

Risk Coordinator Roles and Responsibilities

MMCE & MMCEC are responsible to appointment a Risk Coordinator ("RC") who will be responsible for the roles defined below.

Risk Reporting and Monitoring	<ol style="list-style-type: none"> 1. Coordinate the quarterly risk reporting and monitoring processes at MMCE & MMCEC. 2. Facilitate the identification and assessment of risks to business objectives. 3. Identify and report the critical risks and its current status. 4. Monitor and report the implementation of approved mitigation plans to the RMC. 5. Ensure that appropriate controls are in place by risk owners to manage identified risks including the formulation of preventative and contingency plans where necessary. 6. Check accuracy of information updated in the Enterprise Risk Management System ("ERMS"). 7. Compile and submit company risk report to the company RMC.
Risk Advisory	<ol style="list-style-type: none"> 1. Review, propose and implement an appropriate risk management structure within the Company level. 2. Provide support to the senior management of MMCE & MMCEC in risk issues. 3. Keep abreast of new developments in Group Risk Management. 4. Act as a focal point for all risk management support and advice to the Company. 5. Ensure that full consideration and commentary on risks are provided to support the business strategy and planning cycle.
Risk Communication	<ol style="list-style-type: none"> 1. Communicate enterprise risk management strategies, policies and processes together with defined responsibilities to all management and staff within the Company. 2. Engage in dialogue and discussion with management and staff within the Company to promote risk management awareness and its practical implementation.



	Document Type: POLICY & FRAMEWORK	Document Title: ENTERPRISE RISK MANAGEMENT POLICY & FRAMEWORK	Document Number: MMCE-ERM-001
	Document Owner:		Page: Page 21 of 21
	QUALITY & RISK DEPARTMENT (MMCE & MMCEC)		Revision: Rev. 1
			Date Published: 23 April 2026

APPENDIX 3

Risk Owner Roles and Responsibilities

Risk owners ("RO") identified in each department within MMCE & MMCEC are responsible for the roles defined below: -

Risk Reporting and Monitoring	<ol style="list-style-type: none"> 1. Identify and evaluate risks within the area of responsibility. 2. Ensure that appropriate controls and mitigation plans are in place to manage identified risks. 3. Monitor and report the implementation of approved mitigation plans. 4. Perform monthly compliance and assessment in the ERM risk register ("RR").
Risk Review	<ol style="list-style-type: none"> 1. Identify and evaluate emerging risks within the area of responsibility. 2. Review department's Internal/external audit reports in order to identify issues related risks. 3. Ensure that full consideration and commentary on risk mitigation plans are provided to support business strategy and the planning cycle. 4. Ensure that sufficient budget is available to carry out the relevant mitigation plans and/or existing controls. 5. Update information into the online MMCE & MMCEC Enterprise Risk Management System ("ERMS") / one to one session with RC - if applicable and/or send the RR to RC via email.

