MEDICard PHILIPPINES, INC.

Addendum
Enterprise Risk Management Policy

Document Details

Document Name	MEDICard PHILIPPINES, INC. Risk Management Policy
Document Version	v.1.0
Originating Business Function	Risk and Compliance
Policy Owner	Head of Risk and Compliance
Primary Contact Person	Roy Hipolito
Secondary Contact Person	
Date of First Issuance	12 July 2023
Date of Last Approval	Not Applicable
Version Effective Date	12 July 2023
Implementation Due Date	12 July 2024
Approved by	Medicard Board of Directors
Review Frequency	Once every three years or as needed
Next Review Date	12 July 2026
Document Type *Per Corporate Policy Governance Standard*	Policy
Information Classification *Per Group Data Protection Standard*	Restricted
Related Policies and Standards	AIA Group Risk Management Policy All AIA Risk and Compliance Standards

VERSION CONTROL

Version	Amendments	Approval Date	Approved by
	Initial Version	27 June 2023	Board Risk Committee
		12 July 2023	MediCard Board of Directors

DISTRIBUTION LIST

TITLES
ALL MediCard Employees

Contents

1. Introduction

Risk is inherent in all activities of MEDICard and each member of the organization is responsible for the adoption of sound risk management practices across the organization. The Risk Management process should be an integral part of all business processes of MEDICard to help in the achievement of MEDICard's long term goals and objectives.

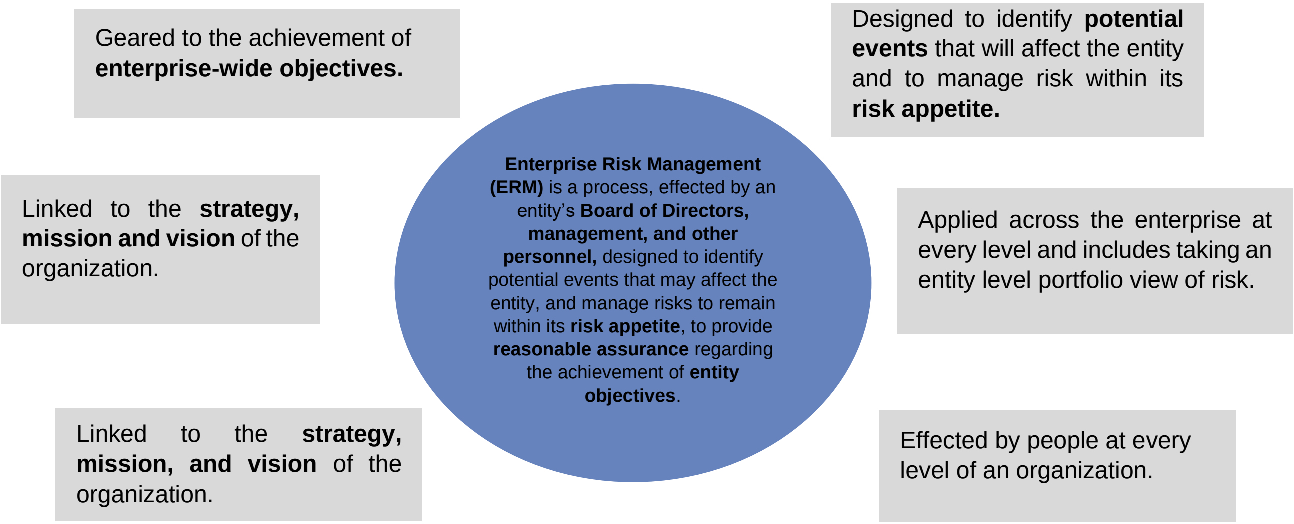
MEDICard acknowledges that risk management is essential to good corporate governance practices. The outputs from successful risk management include strong compliance to regulations and internal policies and procedures, increased assurance on control effectiveness and enhanced decision-making process.

MEDICard recognizes that Enterprise Risk Management aims to provide the structural framework to effectively manage the risks involved in all of its activities. An effective risk management process also provides the opportunity for management to enhance an organization's culture based on ethical values consistent with those expected of MEDICard and its employees. Through this, staff at every level are encouraged to continuously improve performance in addressing the challenges of the organization.

All employees at MEDICard are encouraged to read this document to understand their role in the application of Enterprise-wide Risk Management and cooperate fully with Risk Coordinators, Risk Owners and Audit, Risk & Compliance department while conducting their duties.

2. Purpose

This document provides a framework for Enterprise Risk Management, which typically involves identifying events or circumstances relevant to the organization's objectives, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process. Identifying and proactively addressing risks help the entity to protect and create value for its stakeholders, including employees, regulators, and society overall.



Enterprise Risk Management (ERM) is a process, effected by an entity's **Board of Directors, management, and other personnel,** designed to identify potential events that may affect the entity, and manage risks to remain within its **risk appetite**, to provide **reasonable assurance** regarding the achievement of **entity objectives**.

Geared to the achievement of **enterprise-wide objectives.**

Designed to identify **potential events** that will affect the entity and to manage risk within its **risk appetite.**

Linked to the **strategy, mission and vision** of the organization.

Applied across the enterprise at every level and includes taking an entity level portfolio view of risk.

Linked to the **strategy, mission, and vision** of the organization.

Effected by people at every level of an organization.

3. Approvals and Revisions

Management may add, amend, or delete the contents of any section of this document to align it to the changed circumstances, regulations or proposed new activities at MEDICard. Any employee may recommend changes to this document by referring to their appropriate direct reporting line authority. The policies, practices and procedures contained herein shall be periodically reviewed to achieve the objectives of the ERM activities and to ensure that these are in line with the functions and objectives of the Company.

This document should be formally reviewed by the Board Risk Committee for its completeness, adequacy, and alignment to business imperatives (current and future) at least every three years or on a more frequent basis if deemed necessary.

4. Definitions

Term	Definition
Impact	The outcome or consequence of an event.
Key Risk Indicator (KRI)	An indicator which measures changes in the drivers of risk for a key risk; used to identify a change in inherent risk, which may concurrently produce a change in residual risk if the change in inherent risk is not proportionately mitigated by the control environment.
Key Performance Indicator (KPI)	An indicator which measures or evaluates the success of an organization or of a particular activity (such as projects, programs, products, and other initiatives) in which it engages.
Objectives	Measurable and achievable goals which relate to department/ function or an aspect of one of these.
Risk	A factor, event, or element that creates uncertainty about the ability to meet business objectives.
Risk Rating	The level of risk determined by impact and likelihood.
Risk Register	A formal record of all risks that have been identified.
Threshold	A predefined value for a KPI/KRI set by the management in conjunction with the Risk function of ARC department which provides a warning that a risk may be about to occur or risk exposure is too great. The threshold should align with the risk appetite of the entity and be conservative enough to permit management action to mitigate the risk exposure prior to the risk exceeding limits on risk appetite.

5. ERM Principles

The Enterprise-wide Risk Management (ERM) Framework outlines the aims, intentions, and principles around ERM at MEDICard. For risk management to be effective, MEDICard should at all levels comply with the following principles:

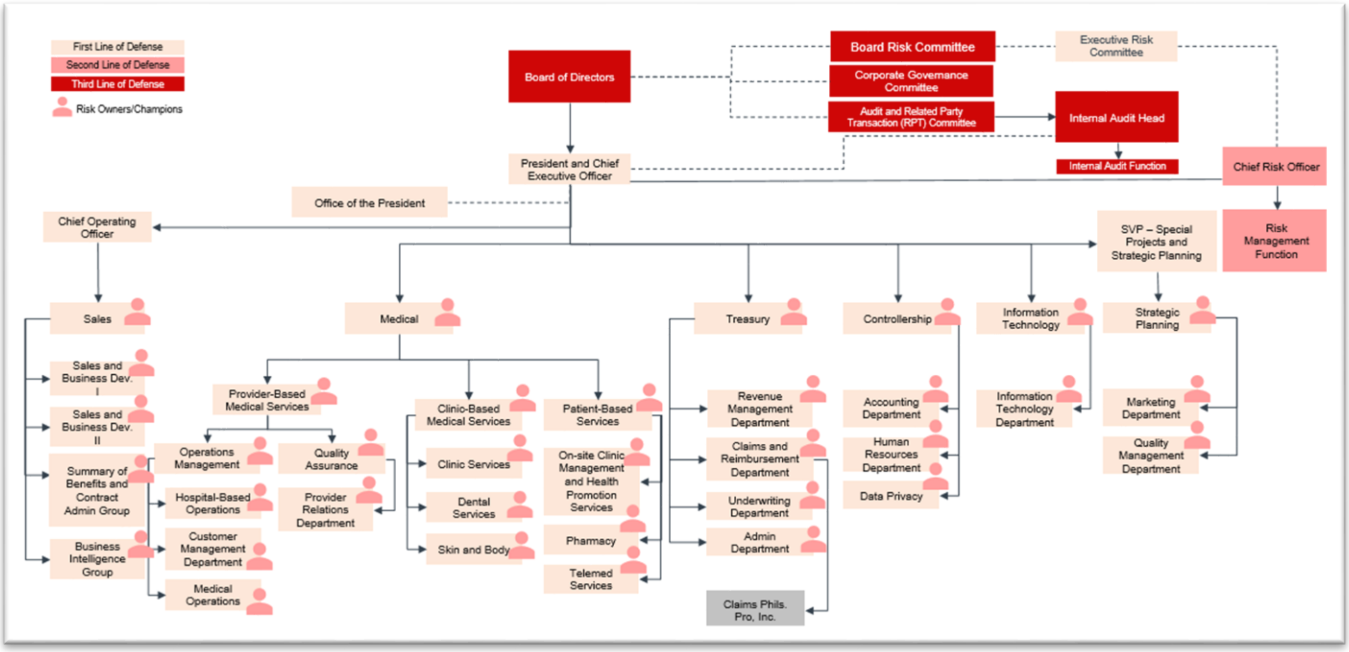
- MEDICard undertakes to establish and maintain an ERM framework within its operations in line with international leading practice.
- MEDICard adopts a structured approach for the management of risks through a process of thorough identification, analysis and cost-effective mitigation and control.
- MEDICard ensures that the full spectrum of risks is managed, including but not limited to, Strategic, Financial, Operational, Legal/ Regulatory and Reputational risks.
- MEDICard sets and maintains a corporate risk appetite for exposure to risks and undertakes to rigorously address all risks above this threshold through risk treatment or termination.
- MEDICard maintains and continuously updates systems for control of significant risks that can adversely impact the delivery of key services.
- MEDICard develops the skills and awareness of its employees in ERM through trainings.

- MEDICard ensures regular measurement, reporting, communication, and review of its ERM framework.
- MEDICard articulates the maximum amount of risk that MEDICard is willing to accept. To achieve the optimal balance of risk and reward that will enable the achievement of MEDICard's strategic objectives. Any risk that breaches the MEDICard risk appetite must be mitigated as a matter of priority to bring it within acceptable levels. For the approved MEDICard's risk appetite, please refer to Risk Appetite Framework.

6. ERM Governance and Responsibilities

6.1 Governance Structure

An effectively functioning oversight structure ensures that risk owners are designated on a timely basis, communication plans are both coherent and capably executed, resources are allocated to risk management and staffing are sufficient, incentives for desired behaviors are in place and, hiring, retention and training practices work as intended. It ensures that managers at all levels are active participants in the risk management process. It also delineates the specific roles and responsibilities of risk-taking versus risk monitoring.


First Line of Defense
Second Line of Defense
Third Line of Defense
Risk Owners/Champions
Board of Directors
Board Risk Committee
Corporate Governance Committee
Audit and Related Party Transaction (RPT) Committee
Executive Risk Committee
Internal Audit Head
Internal Audit Function
Chief Risk Officer
Risk Management Function
President and Chief Executive Officer
Office of the President
Chief Operating Officer
SVP – Special Projects and Strategic Planning
Sales
Medical
Treasury
Controllership
Information Technology
Strategic Planning
Sales and Business Dev. I
Sales and Business Dev. II
Summary of Benefits and Contract Admin Group
Business Intelligence Group
Provider-Based Medical Services
Operations Management
Hospital-Based Operations
Customer Management Department
Medical Operations
Quality Assurance
Provider Relations Department
Clinic-Based Medical Services
Clinic Services
Dental Services
Skin and Body
Patient-Based Services
On-site Clinic Management and Health Promotion Services
Pharmacy
Telemed Services
Revenue Management Department
Claims and Reimbursement Department
Underwriting Department
Admin Department
Claims Phils. Pro, Inc.
Accounting Department
Human Resources Department
Data Privacy
Information Technology Department
Marketing Department
Quality Management Department

(Graph is for Illustrative purposes only)

6.2 Roles and Responsibilities

Board of Directors

The Board of Directors oversees MEDICard's key risks and retains ultimate responsibility for the extent and rigor of risk management activities. The BOD's responsibilities include:

- Ensuring that risk management is implemented across the organization.
- Approving MEDICard's overall risk appetite.

- Receiving the results of any independent appraisals on the adequacy and effectiveness of the risk management framework and process; and
- Reviewing and approving any risk information provided by the Risk Management function.

Audit and Related Party Transaction (RPT) Committee

The Board has established an Audit and RPT Committee to enhance its oversight capability over the Company's financial reporting, internal control system, internal and external audit processes, related party transactions, and compliance with applicable laws and regulations. In relation to the ERM implementation the Audit & RPT Committee shall have the following duties and responsibilities, among others:

- Oversees senior management in establishing and maintaining an adequate, effective and efficient internal control framework, and ensures that systems and processes are designed to provide assurance in areas including reporting, monitoring compliance with laws, regulations and internal policies, efficiency and effectiveness of operations, and safeguarding of assets.
- Through the Internal Audit (IA) Department, monitors and evaluates the adequacy and effectiveness of the Company's internal control system, integrity of financial reporting, and security of physical and information assets; Endorsing any external disclosures that may be required from time to time relating to risk management processes in the organization; and
- Establishes and identifies the reporting line of the Head of Internal Audit to enable him to properly fulfil his duties and responsibilities. For this purpose, the Head of Internal Audit should directly report to the Audit Committee;
- Reviews and monitors Management's responsiveness to the Internal Audit's findings and recommendations;
- Coordinates, monitors and facilitates compliance with laws, rules and regulations;
- Evaluates, on an ongoing basis, existing relations between and among businesses and counterparties;

Executive Risk Committee (Risk Owners)

Risk Owners are department heads or delegated who have been mandated to manage specific risks. Risk Owners are selected based on their knowledge of the risk and their ability to influence controls and treatments associated with that risk. Risk Owners must manage their designated risks in accordance with MEDICard's risk management framework. Their responsibilities include:

- Identifying and assessing risks under their management/ownership.
- Developing and implementing risk response strategies for the risks under their management.
- Monitoring risks and response strategies under their management; and
- Ensuring the accuracy and timeliness of information provided for risk reporting

Chief Executive Officer

The Chief Executive Officer is responsible for:

- Setting MEDICard's risk appetite.
- Reviewing, approving, and monitoring MEDICard's corporate-wide risk register.
- Approving the design and implementation of MEDICard's risk management framework.
- Identifying and escalating relevant corporate risks to the Audit Committee and BOD as required.
- Approving appropriate risk treatment (response) strategies for key corporate risks.
- Ensuring the MEDICard risk management framework is implemented and that risk management is integrated into all business activities and decisions across the organization;
- Reviewing audit results of the risk management processes and taking appropriate actionable decisions.

Risk Management Function

The risk management function is responsible for risk management to the extent of development and coordination of risk management systems and activities including:

- Defining a risk management strategy;
- Identifying and analyzing key risks exposure relating to economic, environmental, social and governance (EESG) factors and the achievement of the Company's strategic objectives;
- Evaluating and categorizing each identified risk using the Company's predefined risk categories and parameters;
- Establishing a risk register with clearly defined, prioritized and residual risks;
- Developing a risk mitigation plan for the most important risks to the Company, as defined by the risk management strategy;
- Communicating and reporting significant risk exposures including business risks (i.e., strategic, compliance, operational, financial and reputational risks), control issues and risk mitigation plan to the Board Risk Committee; and
- Monitoring and evaluating the effectiveness of the Company's risk management processes.

Chief Risk Officer

- Supervises the entire ERM process and spearheads the development, implementation, maintenance and continuous improvement of ERM processes and documentation;
- Communicates the top risks and the status of implementation of risk management strategies and action plans to the Board Risk Committee;
- Collaborates with the CEO in updating and making recommendations to the Board Risk Committee;
- Suggests ERM policies and related guidance, as may be needed; and

- Provides insights on the implementation of the risk management processes, the review of risk measures reported, and compliance with established risk policies and procedures

Risk Managers/Champions

Risk Champions are senior staff of the department who have been nominated and mandated to support the Risk Owners/ Head of Department for maintaining a consistent approach to risk management within their department.

The Risk Coordinator’s role has the following responsibilities:

- Support the identification, management and reporting of risk within their area of responsibility (e.g., department);
- Update and oversee the management of risk register(s) for their area of responsibility.
- Provide risk management updates and support to Risk Owners;
- Support R with regards to risk identification, recording, escalation and management of risk.
- Monitor and follow-up on risk treatment activities and reporting regarding their department; and
- Regularly discuss questions, concerns, opportunities for improvement and training gaps with the Risk Management function.

Internal Audit Function

Internal Audit function has the responsibility to perform the following functions in relation to the risk management function:

- Provides an independent risk-based assurance service to the Board, Audit Committee and Management, focusing on reviewing the effectiveness of the governance and control processes in promoting the right values and ethics; ensuring effective performance management and accounting in the organization; communicating risk and control information; and coordinating the activities and information among the Board, external and internal auditors, and ManagementAssess the implementation of risk treatment strategies.
- Performs regular and special audit as contained in the annual audit plan and/or based on the Company’s risk assessment;
- Performs consulting and advisory services related to governance and control as appropriate for the organization;
- Performs compliance audit of relevant laws, rules and regulations, contractual obligations and other commitments, which could have a significant impact on the organization;
- Reviews, audits and assesses the efficiency and effectiveness of the internal control system of all areas of the company;
- Evaluates operations or programs to ascertain whether results are consistent with established objectives and goals, and whether the operations or programs are being carried out as planned;
- Evaluates specific operations at the request of the Board or Management, as appropriate; and h. Monitors and evaluates governance processes.

Head of Internal Audit

The Head of Internal Audit is Board-appointed and oversee and is responsible for the internal audit activity of the Company and shall directly reports functionally to the Audit Committee and administratively to the CEO. The following are the responsibilities of the Head of Internal Audit, among others:

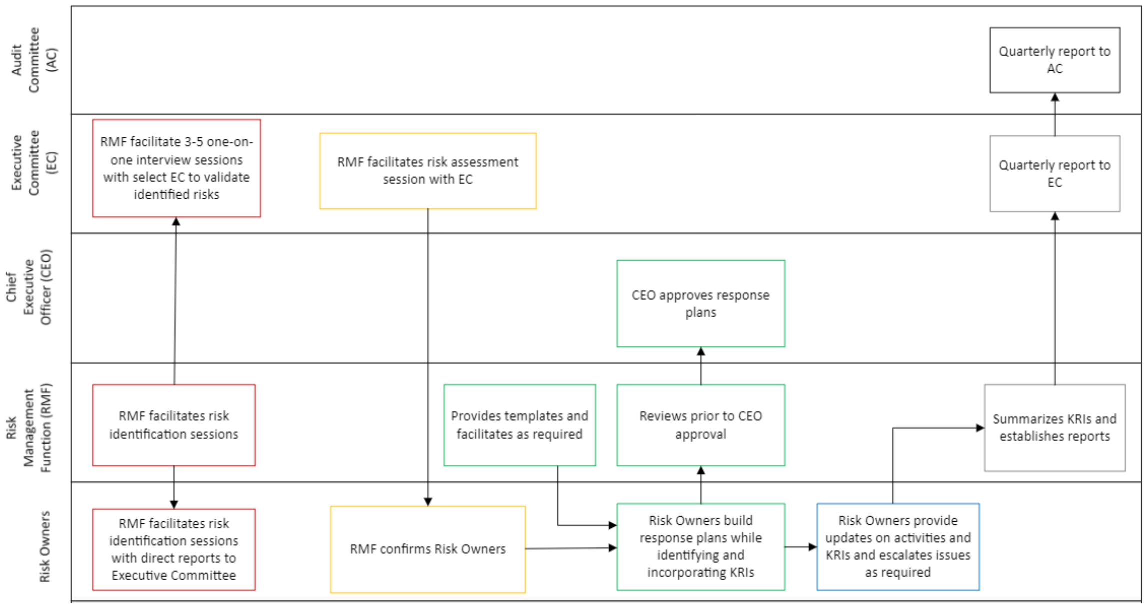
- Periodically reviews the Internal Audit Charter and presents it to senior management and the Board Audit and RPT Committee for approval;
- Establishes a risk-based internal audit plan, including policies and procedures, to determine the priorities of the internal audit activity, consistent with the organization's goals;
- Communicates the internal audit activity's plans, resource requirements and impact of resource limitations, as well as significant interim changes, to senior management and the Audit Committee for review and approval;
- Spearheads the performance of the internal audit activity to ensure it adds value to the organization;
- Reports periodically to the Audit Committee on the internal audit activity's performance relative to its plan; and
- Presents findings and recommendations to the Audit Committee and gives advice to senior management and the Board on how to improve internal processes.

Company staff

All staff have responsibility for managing MEDICard's risks. These include:

- Complying with the risk management framework.
- Being actively involved in risk management activities across the organization.
- Ensuring key risks are identified, reported, recorded, and managed in a timely manner; and
- Receiving appropriate training in risk management

6.3 Process Flow


Audit Committee (AC)
Executive Committee (EC)
Chief Executive Officer (CEO)
Risk Management Function (RMF)
Risk Owners
Quarterly report to AC
RMF facilitate 3-5 one-on-one interview sessions with select EC to validate identified risks
RMF facilitates risk assessment session with EC
Quarterly report to EC
CEO approves response plans
RMF facilitates risk identification sessions
Provides templates and facilitates as required
Reviews prior to CEO approval
Summarizes KRIs and establishes reports
RMF facilitates risk identification sessions with direct reports to Executive Committee
RMF confirms Risk Owners
Risk Owners build response plans while identifying and incorporating KRIs
Risk Owners provide updates on activities and KRIs and escalates issues as required

6.4 ERM RACI

The RACI (Responsible, Accountable, Consulted, and Informed) is a matrix used in the ERM Process to define roles and responsibilities within the organization. It clarifies who is responsible for tasks, who is accountable for their completion, who needs to be consulted, and who needs to be informed.

Here is a breakdown of what each letter in RACI stands for:

Responsible (R): The person or group responsible for completing a specific task or deliverable. This person is accountable for ensuring that the task is completed on time and to the required standard.

Accountable (A): The person who is ultimately accountable for the success of task or decision. This person is responsible for ensuring that the task or decision meets its objectives and that all stakeholders are satisfied with the outcome.

Consulted (C): The person or group who needs to be consulted before a decision is made or a task is completed. These stakeholders provide input and advice based on their expertise or perspective.

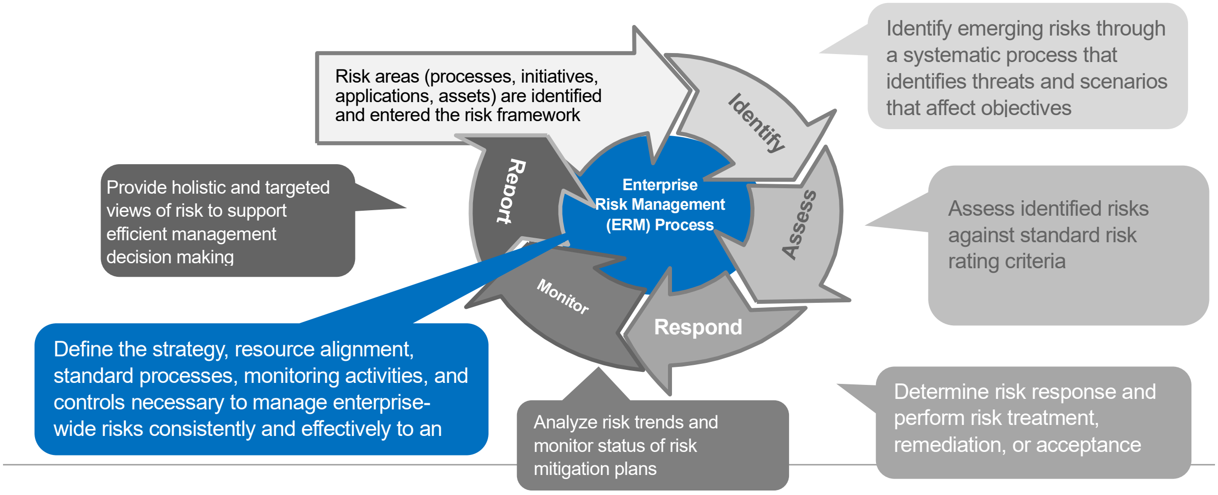
Informed (I): The person or group who needs to be kept informed about the task or decision but does not need to provide input or take action.

Using the RACI framework can improve communication and ensure that everyone involved in the decision-making process understands their role and responsibilities. This can help to avoid confusion, reduce delays, and ensure that decisions are made on time.

ERM Process - RACI						
	Executive Committee (EC)	Chief Executive Officer (CEO)	Risk Management Function (RMF)	1st LoD	2nd LoD	3rd LoD
Risk Identification						
Scan environment for emerging and known risks			A/R	C	C	C
Facilitate risk identification sessions with direct reports to EC			A/R	C	C	C
3-5 one-on-one interview sessions with select EC to validate identified risks	C		A/R			
Approve a comprehensive list of risks	C	A	R			C
Risk Assessment						
Facilitate a risk assessment session with EC	C		A/R			
Confirm risk owners	C	C	A/R	I	I	I
Risk Response Planning						
Develop risk response plans	I	C	A	R	R	R
Risk Monitoring						
Track activities, monitor KRIs, and escalate issues as required	I	I	A	R	R	R
Risk Reporting						
Develop reports	I	I	A/R	C	C	C
Escalate relevant risks to the relevant committee	I	A	R			I
Determine additional mitigation actions to resolve issues as required	A	C	R	C	C	C

7. ERM Framework

The overview of the risk management process that will be undertaken within MEDICard is shown in the following diagram:



Risk areas (processes, initiatives, applications, assets) are identified and entered the risk framework
Identify emerging risks through a systematic process that identifies threats and scenarios that affect objectives
Identify
Provide holistic and targeted views of risk to support efficient management decision making
Report
Enterprise Risk Management (ERM) Process
Assess
Assess identified risks against standard risk rating criteria
Monitor
Respond
Define the strategy, resource alignment, standard processes, monitoring activities, and controls necessary to manage enterprise-wide risks consistently and effectively to an
Analyze risk trends and monitor status of risk mitigation plans
Determine risk response and perform risk treatment, remediation, or acceptance

7.2 Risk Identification

Risk Identification is to identify and report on enterprise risks across the company that could impact the achievement of strategic goals and objectives. Those risks could be operational or financial.

Key activities include engaging the business unit / functional unit leaders to understand and document including:

- Identify and report risks and/or opportunities to the achievement of strategic goals and objectives
- Think broadly and consider risks and opportunities within the operational and financial risk categories identified in the MEDICard Risk Landscape.
- Collect and document key risk information, including:
  - The risk
  - Definition of the risk (scenario)
  - Root cause(s) of the risk/opportunity
  - How risk/opportunity impacts performance
  - Current and/or potential mitigation efforts

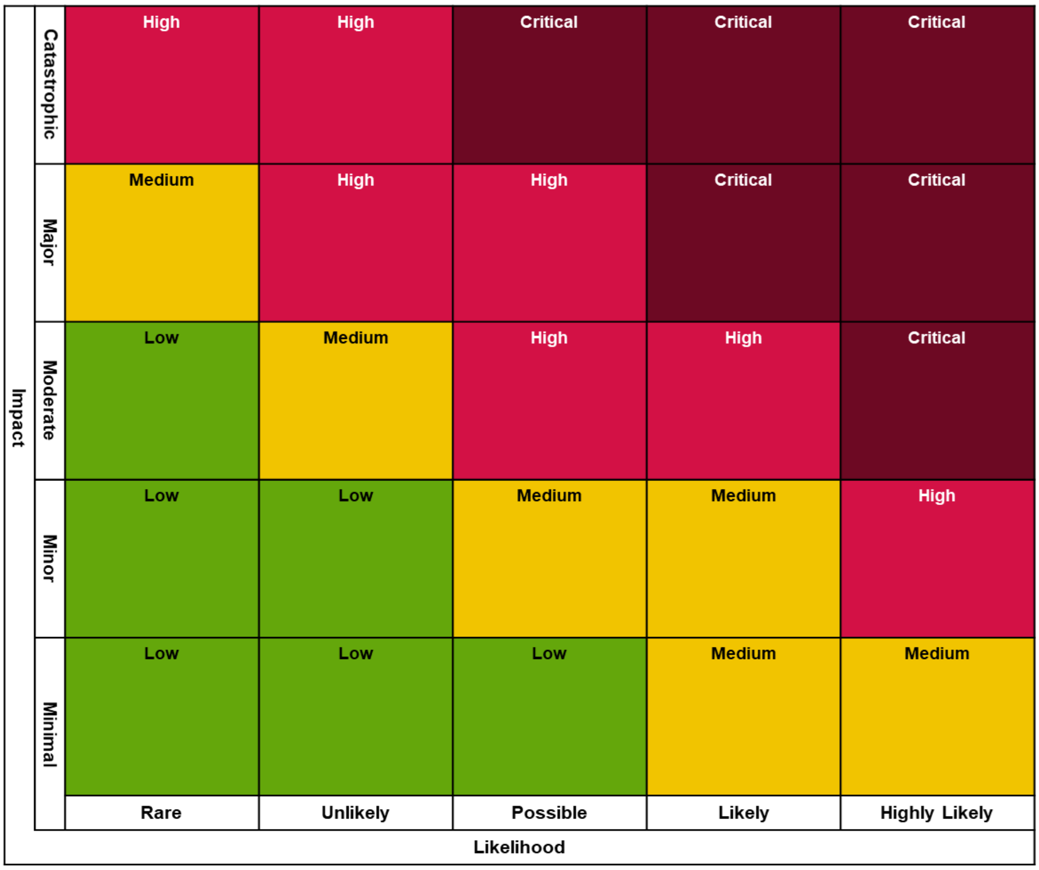
Risk identification can be enabled through several platforms such as the Teams digital channel, to conduct a facilitated real time feedback session from key stakeholders within the company.

Resulting outputs from this session include: summary of the risks identified during the risk identification session(s)., with unique risk names, a summary of risk drivers for each unique risk and current and potential mitigation. This information is used to jumpstart the risk prioritization and risk assessment process.

7.3 Risk Assessment

Risk Assessment as part of the ERM process involves assessing the nature and characteristics of each risk and determining its significance based on its likelihood (probability) and potential impact to the company.

Based on the results of the risk assessment, the company will be able to prioritize and develop strategies to manage or mitigate the risks.



Impact						
	Catastrophic	High	High	Critical	Critical	Critical
	Major	Medium	High	High	Critical	Critical
	Moderate	Low	Medium	High	High	Critical
	Minor	Low	Low	Medium	Medium	High
	Minimal	Low	Low	Low	Medium	Medium
		Rare	Unlikely	Possible	Likely	Highly Likely
		Likelihood				

Risk Rating Matrix

Following the principles of the ***AIA Group Operational and Control Standard***, the Risk Assessment Matrix is the tool used to visually represent and categorize the risks based on their impact (y axis) and likelihood (x axis) levels. It is utilized to assess and quantify the risks involved in the daily activities of a business and classifying them (low, medium, high, and extreme) by assigning numerical values to represent their impact on the business.

Following the scale of low to high, the 5x5 Risk Matrix assigns 5 categories each for likelihood and impact categories in assessing the risks.

Likelihood

This parameter in the Risk Assessment Matrix asks the question: ***How likely is the risk to happen?***

Scale	Description	Qualitative-based Probability of Occurrence
5	Highly Likely	The event is expected to occur in most circumstances; or 75% or greater chance of occurrence over the life of the asset or project
4	Likely	The event will probably occur in most circumstances; or 50% up to 75% chance of occurrence over the life of the asset or project
3	Possible	The event will possibly occur at some time; or 25% up to 50% chance of occurrence over the life of the asset or project
2	Unlikely	The event may occur in exceptional circumstances; or 5% up to 25% chance of occurrence over the life of the asset or project
1	Rare	The event is unlikely to occur; or <5% chance of occurrence over the life of the asset or project

Impact

This parameter in the Risk Rating Matrix asks the question: ***How severe would the outcome/s be if the risk occurred?*** Impact is assessed in monetary terms and thresholds approved by the Board of Directors where possible and classified per the table below.

Scale	Description	Direct / Indirect Financial / Operational Loss*	Fines and Sanctions	Customer Outcome	Business Disruption/ Physical Security	Reputation	Impact to Strategy / Business Model	Impact to Financial Reporting
5	Catastrophic	Direct loss or increased cost of greater than: 5% of Local OPAT or greater than USD40m	Significant prosecution and fines, litigation including class actions, punitive action of accountable individuals or closure of business	Widespread extreme customer detriment and/or systemic negative market impact	Significant operations/services disruption to multiple critical functions/services across one/more business areas, or multiple fatalities to employees or third parties	International long-term negative media coverage with game-changing loss of market share	Internal or external event that can lead to a long-term material impact to MPI's strategy and/or business model	Misstatement of greater than Materiality Threshold as referenced in the Group Finance Materiality Framework
4	Major	Direct loss or increased cost of up to 5% of Local OPAT or between USD20m to USD40m	Multiple material Breaches reportable to the local regulator or major project for corrective action	Significant detriment to a large group of customers	Limited operations/services disruption to critical functions or services, or single fatality/multiple serious injuries to employees or third parties	International short-term or national long-term negative media coverage causing significant loss in market share and shareholder support	Internal or external event that can lead to a medium-term material impact to MPI's strategy and/or business model	Misstatement of up to 100% of Materiality Threshold as referenced in the AIA Group Finance Materiality Framework
3	Moderate	Direct loss or increased cost of up to 3% of Local OPAT or between USD8m to USD20m	Multiple related minor Breaches reportable to the local regulator with immediate correction to be implemented	Moderate detriment to a large group of customers	Operations/services disruption to multiple non-critical functions or services across one/more business areas, or some serious injuries to employees or third parties	National short-term negative media coverage causing decreased support from shareholders or the community	Internal or external event that can lead to a short-term material impact to MPI's strategy and/or business model	Misstatement of up to 70% of Materiality Threshold as referenced in the AIA Group Finance Materiality Framework
2	Minor	Direct loss or increased cost of up to 1% of Local OPAT or between USD4m to USD8m	A few non-systemic Breaches or reportable Incidents with no follow up correction required	Moderate detriment to a large group of customers	Operations/services disruption to multiple non-critical functions or services across one/more business areas, or some serious injuries to employees or third parties	National short-term negative media coverage causing decreased support from shareholders or the community	Internal or external event that can lead to a short-term material impact to MPI's strategy and/or business model	Misstatement of up to 70% of Materiality Threshold as referenced in the AIA Group Finance Materiality Framework
1	Minimal	Direct loss or increased cost of up to 0.5% of Local OPAT or up to USD4m	Non-systematic Breaches with no adverse impact or not reportable to regulator	Minor detriment to a small group of customers	Limited operations/services disruption to a non-critical function/service, or no injuries to employees or third parties	Local media attention is quickly remedied with public awareness but not concern	Internal or external event that can lead to an immaterial impact to MPI's strategy and/or business model	Misstatement of up to 20% of Materiality Threshold as referenced in the AIA Group Finance Materiality Framework

**Note: Assuming a conversion rate of USD 1: PHP 56 as of May 30, 2023.*

To get the Risk Level, the two parameters are multiplied.

Likelihood x Impact = Risk Level

The Risk will then be categorized based on the range the Risk Level falls under.

Risk Level	Rating	Description
1-4	Low	Risks that are unlikely to occur and would have little to no impact to the business.
5-8	Medium	Somewhat likely to occur, these risks come with slightly more serious consequences. If possible, the company should take steps to prevent medium risks from occurring.
9-12	High	These are serious risks that both have significant consequences and are likely to occur. Risks that are once identified, should be actioned upon in the near term.
13-25	Critical	Catastrophic risks that have severe consequences and are highly likely to occur. Extreme risks are the highest priority and must be responded to immediately, as they can threaten the success of the company.

7.4 Risk Response

Risk response is a critical component of risk management. The objective of risk response is to minimize the negative impact of identified risks on the company and maximize the positive impact of opportunities. MEDICard can take four main strategies for risk response: avoid, mitigate, transfer, and accept.

Avoiding Risks

Avoiding risks is the most effective risk response strategy. This involves identifying risks that can have a significant impact and taking steps to eliminate them. Avoiding risks can be done by complete elimination of the risk through changes in the company’s operations, products, or processes. For example, MEDICard can avoid risk through careful selection of its affiliate healthcare providers and only work with those who have a proven track record of success and low rates of medical errors. By doing this, the company can reduce the harm to patients and limit exposure to liability.

While avoiding risk can be an effective strategy for mitigating potential harm, it's important to carefully weigh the potential benefits and drawbacks of this approach. In some cases, it may be more beneficial to pursue risk management strategies that allow for greater flexibility and opportunity while still minimizing potential risk. For example, limiting coverage or excluding certain procedures that have a high risk of complications can reduce the risk of medical malpractice and liabilities, however, this may also lead to dissatisfaction among members and limit MEDICard’s ability to provide comprehensive care.

Mitigating Risks

Mitigating risks involves taking proactive steps in reducing the likelihood and/or impact of the identified risks. This can be achieved by through implementing the following preventive measures:

1. **Process improvement:** This involves systematic review of existing processes, identifying areas that need improvement, and developing and implementing solutions to address those

areas. Moreover, implementing process improvements, such as standard operating procedures or workflow modifications, can help reduce the risk of errors or other issues.

Another benefit of process improvement is that it can help to identify and prevent potential sources of risk before they become a problem. For example, by analyzing data from previous incidents, the company can identify patterns and trends that may indicate underlying issues within a process. By addressing these issues proactively, the company can prevent incidents from occurring in the future.

2. **Quality control:** Quality control refers to the processes and procedures used to ensure that products or services meet or exceed member expectations and industry standards. By implementing a quality control program, the company can minimize the risk of errors and other issues that can lead to member complaints, additional costs, or damage to the company's reputation.

   One of the key components of quality control is the establishment of quality standards. Quality standards are a set of criteria that define the minimum acceptable level of quality for a product or service. In terms of clinical services, these standards can be based on industry regulations or patient requirements.

3. **Contingency planning:** The goal of contingency planning is to minimize the impact of an incident by enabling the company to respond quickly and effectively. It involves identifying potential incidents, assessing the likelihood and potential impact of each incident, and developing response strategies for each incident.

   Response strategies may include procedures for evacuating personnel, securing assets, and communicating with stakeholders. By developing and regularly updating a contingency plan, the company can ensure that they are prepared to respond to a wide range of incidents, including natural disasters, cyberattacks, and other emergencies.

It is important to remember that mitigation strategies are often used when avoiding risks is not feasible or when the cost of avoiding risks is too high.

Transferring Risks

Transferring risks involves transferring the risk to another party. This can be achieved through third-party contracts or outsourcing. Transferring risks is often used when the company does not have the expertise or resources to manage the risk effectively. When transferring risks, the company is essentially paying another party to assume the potential financial or other consequences of the risk. By doing so, the company can mitigate the impact of the risk on its own operations and reduce its exposure to potential losses.

Accepting Risks

Accepting risks is a risk response strategy that involves acknowledging the existence of a risk and choosing not to take any additional action beyond monitoring it. This strategy is typically used for risks that are deemed acceptable, either because the likelihood of the risk occurring is low or because the potential impact of the risk is relatively minor. This is often done when the cost of mitigating the risk outweighs the potential impact.

Accepting risks is not a passive approach to risk management; it requires active management and monitoring of the risk. Additionally, it is important to ensure that the decision to accept a risk is made based on a thorough understanding of the risk and its potential consequences, and that it is consistent with the company's risk tolerance and overall risk management strategy.

7.5 RISK MONITORING

Risk monitoring is the continuous process of tracking identified risks and evaluating the effectiveness of risk responses. The objective of risk monitoring is to ensure that the risk management plan in place is effective, and MEDICard is on track to achieve its objectives. The key steps involved in risk monitoring are:

1. Identifying new risks: Risk monitoring involves continuous tracking of existing/identified risks and keeping an eye out for potential risks that may arise resulting from changes in the risk environment, new threats, or changes in the likelihood or impact of existing risks. This data can be collected through a variety of sources, such as internal reports, external market research, and data analytics.

2. Assessing the effectiveness of existing risk responses: This involves evaluating the effectiveness of existing risk responses and modifying them as needed. If the risk response strategy is not effective, the company should consider a new risk response strategy.

3. Updating the risk management plan: This involves updating the risk management plan to reflect any changes in the MEDICard Risk Landscape. The Risk Management Plan should be updated regularly to ensure that it remains relevant and effective. Following the Risk Management Framework, the Risk Champions shall conduct Functional Unit Risk Management Meetings (FuRMMs) in order to properly document risk incidents, outstanding risks and measures taken, and identify new or emerging factors for risks.

4. Communicating risk status: This involves communicating to stakeholders such as senior management and key decision-makers, information on the identified risks, their potential impact on the company, progress of risk management activities, and/or any recommended actions to mitigate or manage the risks.

7.6 RISK REPORTING

Risk reporting is the process of communicating information about identified risks and risk responses to stakeholders. The objective of risk reporting is to provide stakeholders with the information they need to make informed decisions. The key steps involved in risk reporting are:

1. **Identifying the audience:** This involves identifying the stakeholders who need to receive information about identified risks and risk responses. The audience can include senior management, key decision-makers, members, and regulators. Different stakeholders may have different needs and expectations for risk information, so it is important to tailor the communication to the needs of each stakeholders group.
2. **Determining the frequency of reporting:** This involves determining how often risk information should be communicated to stakeholders. The frequency of reporting should be based on the level of risk and the needs of the stakeholders. Reports should be produced on a regular basis, such as monthly or quarterly, and must present a summary of the key existing risks as well as potential risks that may arise due to changes in the internal and external environment of the company.

3. **Selecting the format:** This involves selecting the format in which risk information will be communicated to stakeholders. The format can include written reports, dashboards, and presentations. The report should also outline the key metrics and indicators that will be monitored and reported on, such as the level of risk exposure, the effectiveness of risk controls, and the status of risk mitigation and management activities.
4. **Communicating the risk information:** This involves communicating the risk information to stakeholders in a clear and concise manner. The communication should also be transparent, providing stakeholders with the full picture of the risks facing the organization.

8. Delegation of Authority

In line with the Group's principle of 'empowerment within a framework', the Group CRO delegates authority for implementing the requirements of this Policy and addendum within each BU to the relevant BU CRO. MEDICard Philippines Inc. CRO is further empowered to delegate authority to their direct reports, or as otherwise deemed appropriate.

CRO is responsible for reporting any matters to the Group CRO as they would reasonably expect to be made aware of, including but not limited to any exemptions and breaches to this Policy.

Notwithstanding the above, responsibility for the overall design and execution of the RMF and other Policy requirements sits with the Group CRO. The Group BRC, with the support of Group ERC, is ultimately accountable for the Group RMF, on behalf of the Group Board.

The latest effective version of this Policy shall reside on the CPP as per the CPG Standard. Any inquiries of this Policy shall be made to the primary policy contact person as listed in the CPP and stated in the document details section of this Policy.

9. Approvals

This Policy is approved by the MediCard Board. Prior to approval, this Policy is endorsement by the CRO and Board Risk Committee at a minimum.