MAXICARE HEALTHCARE CORPORATION

MINUTES OF THE MEETING OF THE BOARD RISK OVERSIGHT COMMITTEE

Boardroom, Maxicare Tower
203 Salcedo Street, Legaspi Village, Makati City[1]
20 December 2024, 3:00 P.M.

PRESENT:

RICARDO V. MARTIN
ENRICO S. CRUZ
TEODORO M. PANGANIBAN
RIZALINA MANTARING

ALSO PRESENT:

RENE J. BUENAVENTURA
BRIAN M. GO
CHRISTIAN S. ARGOS
ELLIE DE GUZMAN
MICA SALAZAR
GLADICE CENSON
ATTY. ANDREW FORNIER
ATTY. DANNY E. BUNYI
ATTY. MARY ZOELLI R. VELASCO
RIZ GAURAN

I. CALL TO ORDER AND DETERMINATION OF QUORUM

The Broad Risk Oversight Committee (the "**Committee**") Chairperson, Mr. Ricardo V. Martin, ("**Mr. Martin**") called the meeting to order. The Corporate Secretary, Atty. Danny E. Bunyi ("**Atty. Bunyi**"), recorded the Minutes of the proceedings.

Atty. Bunyi certified that notices were sent to all the members of the Committee in accordance with Maxicare Healthcare Corporation's (the "**Corporation**", "**Maxicare**", or "**MHC**") By-Laws and he certified the existence of a quorum for the transaction of business at hand.

[1] The meeting was conducted virtually through video conferencing (Zoom Video Conferencing) pursuant to Securities and Exchange Commission Memorandum Circular No. 6-2020, dated 12 March 2020, and the Corporation's duly adopted Internal Procedures for the Conduct of the Board and Shareholders' Meetings.

II. APPROVAL OF THE MINUTES OF THE PREVIOUS MEETING

The Minutes of the last Committee meeting held on 29 August 2024 was presented to the members for approval, a copy of which was previously distributed to the members of the Committee. Upon motion duly made and duly seconded, the Minutes of the Meeting held on 29 August 2024 was approved.

III. MATTERS ARISING FROM THE MINUTES

Summarized below are the following items that arose from this Committee meeting. A separate sheet indicating the same is likewise attached to this file as Annex "**A**":

A. *Heat Map – Monetary Value*

A detailed narration of assigning monetary values to certain risk categories in the heat map is indicated in the succeeding of sections these Minutes. Among the suggestions was to add values in the various risk categories. It was also proposed that thresholds be incorporated for every level of risk. A post-treatment chart of the heat map was likewise requested once the indicated risks have been down to zero.

B. *Specific Examples of the High-Level Risk*

Specific examples on high-level of risk were asked by the Committee, which the Legal and Risk Compliance deferred to the head of the Quality Management System.

C. *Reporting of the Risk Items and Risk Dashboard*

It was noted that the actual number of risks as reflected in the risk map were voluminous. To address this, risk grouping was suggested.

D. *Incident Notification*

It was proposed that the Committee and the Board of Directors be given a notification in case there are high-level risks or incidents of high public interest (i.e. data breach) to apprise the Committee and the Board of the incident. There was also a suggestion to provide the Committee and the Board of Directors the script to answer any external inquiries.

E. Detailed Report on the High-Level Risk

It was proposed that a complimentary discussion of the top risks be provided alongside the heat map. A focused discussion of the red items and how it should be addressed based on company policy must likewise be made. Additionally, it was suggested that the top 10 risks be reported every meeting.

F. Residual Risk Report

It was proposed that a post-treatment risk report should be done. The Committee requested a presentation that focuses on residual risks rather than the initial risk levels. This shift in focus would provide a more accurate and actionable understanding of the current risk landscape, as mitigation efforts may have significantly altered the initial risk levels.

This proposal also emphasized the importance of understanding the current risk profile after considering the impact of implemented mitigation strategies. A worksheet detailing former high risks which have been decreased to lower residual risks due to mitigation strategies was requested.

G. Report on the Recovery Point of Objective ("RPO") of IT

First, it was proposed that a future meeting dedicate a portion to a detailed discussion of the IT recovery process, covering crucial aspects such as backup strategies, including offsite backups, to ensure a comprehensive understanding of the critical role IT plays in business continuity. Second, the Committee proposed that the discussion on risk mitigation should address the impact of application, system, or data center outages, examining the specific protections in place to mitigate the risks associated with such disruptions. These proposals aim to enhance the Committee's understanding of critical IT recovery processes and the specific mitigation strategies to address potential disruptions. Third, it was noted that even if an application can be restored quickly (e.g., within two hours), significant data loss can severely impact a department's ability to function effectively. As such departments must define their RPOs, specifying the maximum data loss in terms of time (e.g., one hour, one day, one week). This ensures that data recovery aligns with business needs and minimizes disruption to operations.

H. Call Tree Testing

The Committee proposed two measures to enhance the effectiveness of the emergency contact list. First, it was suggested that regular tests be conducted to evaluate the response times of the emergency contact list. Second, the Committee recommended recording the number of responses received during each test and their corresponding response times to track the overall effectiveness of the emergency contact list. These proposals aim to ensure the timely and effective activation of emergency response procedures.

I. Crisis Management Team and Business Continuity Team

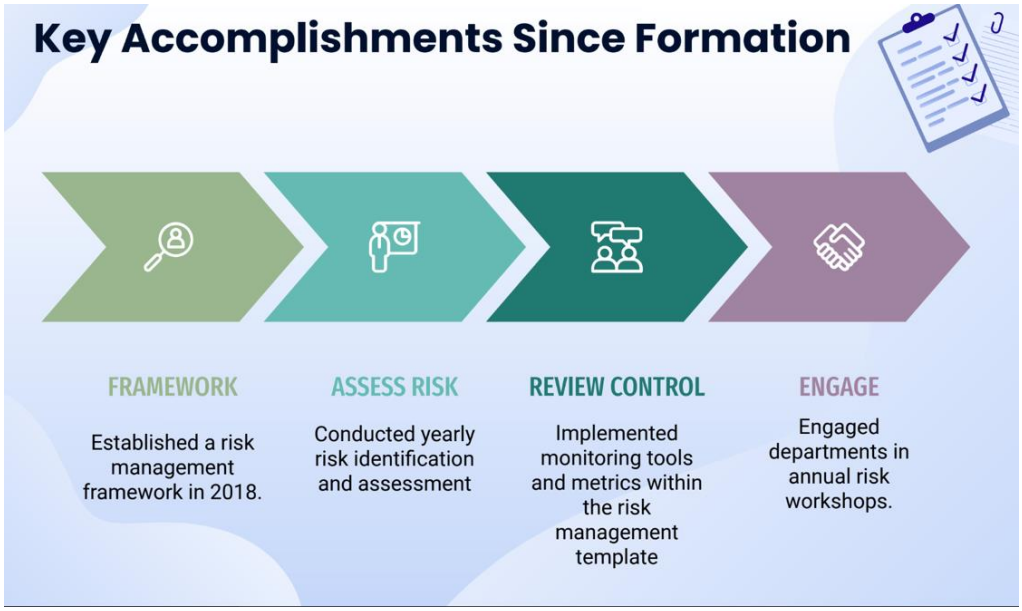
The Committee suggested that the next step in enhancing business continuity awareness is to educate all employees on the existence and roles of the Business Continuity Committee and the Crisis Committee. This proposal aims to increase employee awareness of the available resources and support systems in the event of a crisis.

IV. ENTERPRISE RISK MANAGEMENT FRAMEWORK

Atty. Andrew Fornier ("**Atty. Fornier**"), the Maxicare Group Legal and Risk Compliance Officer reported the current developments for the Enterprise Risk Management ("**ERM**") Framework.

First, Atty. Fornier provided a brief background on the current ERM Framework. He explained that the existing ERM framework was established in 2018 and that it is currently placed under the quality management system ("**QMS**") department, which is now under Legal Risk and Compliance as of 2024.

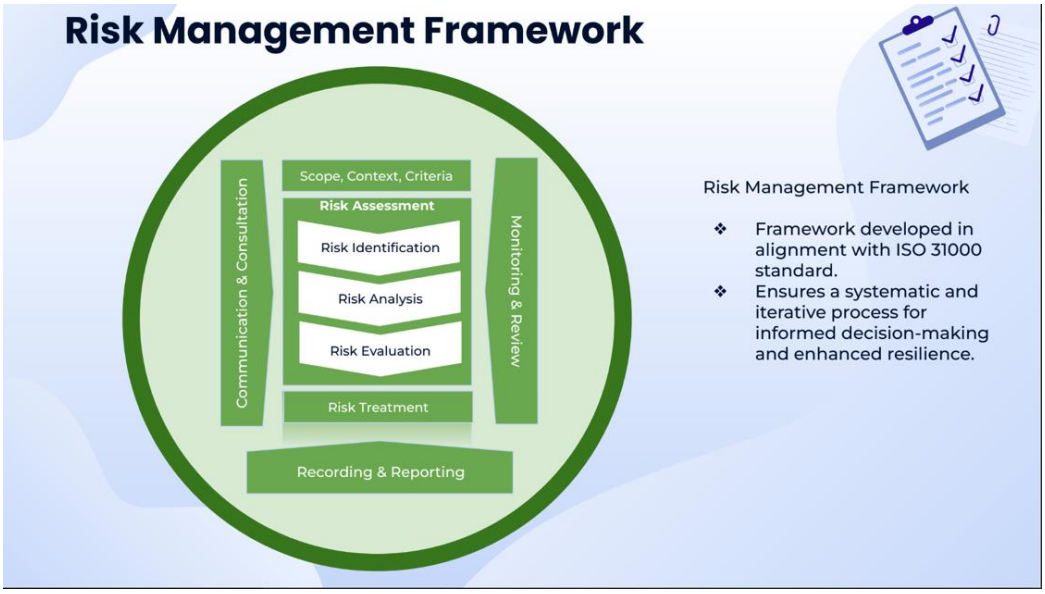
He discussed the key accomplishments of the ERM since it was formed:



According to Atty. Fornier, the team adopts, assesses, and identifies risk on an annual basis. This was done in conjunction with the various departments and stakeholders, as well as assessment of the same. There is also a review of the risk management template. There was a certain process involved in identifying the risks in terms of likelihood and impact, as well as with other aspects, relevant aspects regarding risk management. These were then eventually incorporated into the risk treatment procedures, as well as correctional corrective action schedules.

Atty. Fornier explained that there was reporting done between QMS, which was the body responsible for maintaining and monitoring the risk management, and the various departments of Maxicare which were also invested in identifying the risk and analyzing the same and incorporating the treatment of these risks in their various operations and strategies.

On an annual basis, each department is invited by QMS to participate in a risk workshop where various risks are identified, reanalyzed, and updated accordingly. In every year of this exercise, Maxicare had a more accurate picture of the current risk framework of the Corporation. The risks that may have been identified as high risk previously with proper treatment will have been mitigated and perhaps replaced by new risks that have emerged based on the existing environment.



The current risk management framework was adapted from ISO 31000. Unlike other ISOs that Maxicare had applied for certification in the past, such as ISO 27000, ISO 31000 is not a certification program. It is merely a set of guidelines that were created by the ISO network in order to operationalize and provide some formal structure to risk management at an enterprise level. It involves a detailed process of risk assessment, and then treatment of those risks, monitoring and review on a periodic basis of these risks, as well as recording and regular reporting to relevant bodies to provide guidance on how risk management.

Atty. Fornier similarly emphasized the importance of the element of communication and consultation, both with top management and various invested departments to ensure that the ERM framework remains up to-date and responsive to the changes in the business environment of Maxicare.

Mr. Teodoro Panganiban ("**Mr. Panganiban**") expressed his desire to understand which aspects of the ERM framework were currently in place and which are not yet implemented. He requested clarification on the framework, specifically identifying the components with established processes and those still under development. Additionally, he inquired about the intended timeline for implementing the remaining components.

Atty. Fornier confirmed that all the systems that were being presented were in place as of the current set-up. Nonetheless, he explained that while every system was in place, he would be discussing the challenges of the current ERM framework, which would be consulted with the Committee. He likewise clarified that the systems being discussed were not just policies in place but

were being implemented within the Corporation. He said that all functions such as identification, analysis, evaluation, corrective action, and consultation were in place. However, there were some challenges in the current framework with respect to reporting.

Mr. Panganiban then asked who was responsible for the monitoring and review under the ERM framework. Atty. Fornier responded that the system was primarily under the guidance of QMS, which was under the Legal Risk and Compliance ("**LRC**") of Maxicare. QMS has been responsible for managing the framework over the past five or six years. It is QMS's primary responsibility to ensure that the framework was followed and adopted. It is concurrently the responsibility of each department involved to ensure that the risks are properly analyzed and identified; and if there were any corrective actions that need to be taken to mitigate or treat the risk. Also, it is concurrently the responsibility of each department involved to ensure these actions are effectively taken and the results of those treatment activities are reported to the QMS for further monitoring. He further explained that QMS releases an annual report detailing the opportunities and risk assessment of the Corporation. He explained that the monitoring and review of the risks was broken down into every minute detail, likelihoods, impacts, and other elements of each identified risk. However, Atty. Fornier recognized that there were certain limitations in the process that can be improved.

Mr. Panganiban also commended the current system for having a database of risks identified and being monitored and treated.

Atty. Fornier then presented and discussed the policy that Maxicare currently follows with regard to opportunity and risk assessment:

First, risks are identified by each department through an examination of their processes, policies, and key risk areas that may be detrimental to their operations and efficiency.

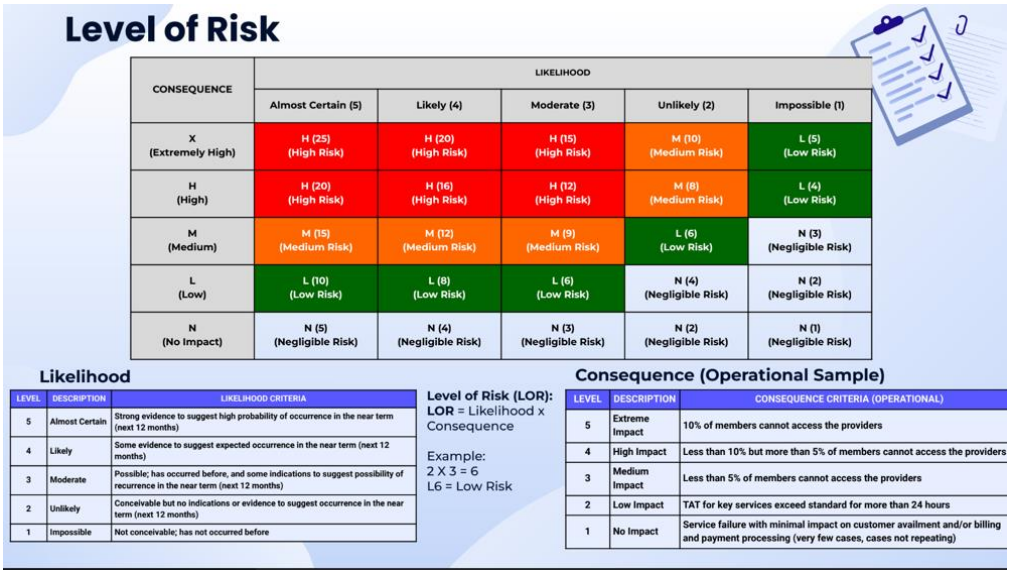
Second, these identified risks are analyzed based on both their likelihood and impact. Likelihood refers to the probability of the risk event occurring, while impact assesses the severity of its potential consequences on the business.

Third, these risks are evaluated against existing controls. Initially, each risk is assessed independently, followed by a comparison against the company's existing checks and balances, control features, and other risk treatment measures currently undertaken by the Corporation. While some risks may initially appear to have high impact, the presence of existing policies, processes, or actions can significantly mitigate them. These mitigated risks are then cataloged or databased and do not require further immediate action.

Fourth, for risks requiring further action, appropriate controls, solutions, and action plans are developed in collaboration with the concerned departments.

Fifth and finally, these risks are monitored over a specific timeframe, typically between six months to one year. The QMS and the concerned department jointly assess the effectiveness of the implemented treatment options or mitigating actions in managing the identified risks. This risk assessment and management process is conducted annually across all departments and for all identified risks.

Atty. Fornier presented the Level of Risk heat map to the Committee:



Level of Risk

CONSEQUENCE	LIKELIHOOD				
	Almost Certain (5)	Likely (4)	Moderate (3)	Unlikely (2)	Impossible (1)
X (Extremely High)	H (25) (High Risk)	H (20) (High Risk)	H (15) (High Risk)	M (10) (Medium Risk)	L (5) (Low Risk)
H (High)	H (20) (High Risk)	H (16) (High Risk)	H (12) (High Risk)	M (8) (Medium Risk)	L (4) (Low Risk)
M (Medium)	M (15) (Medium Risk)	M (12) (Medium Risk)	M (9) (Medium Risk)	L (6) (Low Risk)	N (3) (Negligible Risk)
L (Low)	L (10) (Low Risk)	L (8) (Low Risk)	L (6) (Low Risk)	N (4) (Negligible Risk)	N (2) (Negligible Risk)
N (No Impact)	N (5) (Negligible Risk)	N (4) (Negligible Risk)	N (3) (Negligible Risk)	N (2) (Negligible Risk)	N (1) (Negligible Risk)

Likelihood

LEVEL	DESCRIPTION	LIKELIHOOD CRITERIA
5	Almost Certain	Strong evidence to suggest high probability of occurrence in the near term (next 12 months)
4	Likely	Some evidence to suggest expected occurrence in the near term (next 12 months)
3	Moderate	Possible; has occurred before, and some indications to suggest possibility of recurrence in the near term (next 12 months)
2	Unlikely	Conceivable but no indications or evidence to suggest occurrence in the near term (next 12 months)
1	Impossible	Not conceivable; has not occurred before

Level of Risk (LOR):
LOR = Likelihood x Consequence

Example:
2 X 3 = 6
L6 = Low Risk

Consequence (Operational Sample)

LEVEL	DESCRIPTION	CONSEQUENCE CRITERIA (OPERATIONAL)
5	Extreme Impact	10% of members cannot access the providers
4	High Impact	Less than 10% but more than 5% of members cannot access the providers
3	Medium Impact	Less than 5% of members cannot access the providers
2	Low Impact	TAT for key services exceed standard for more than 24 hours
1	No Impact	Service failure with minimal impact on customer availment and/or billing and payment processing (very few cases, cases not repeating)

Atty. Fornier explained that the risks have been categorized based on their likelihood and consequence (or impact). Previously, a high-medium-low scale was used, but this had been expanded to accommodate a wider range of risk types and mitigation strategies.

He noted that the current likelihood and consequence criteria may require adjustment. Some risks, while not affecting a large percentage of members, can still have a significant impact, particularly on reputation. Even a 1% impact on members can be highly damaging in certain cases. Therefore, a more refined approach may be necessary, potentially involving a category-specific assessment of likelihood and impact instead of a general evaluation.

Ms. Rizalina Mantaring ("**Ms. Mantaring**") suggested adding monetary values and assigning it to various risk categories. She noted that some organizations assign monetary values to assess the impact of risks, such as low, medium, high, or extreme. This would also aid in data comparison.

Atty. Fornier acknowledged that assigning monetary values to certain risk categories, such as financial or operational risks, is an area for refinement. He recognized that the current likelihood and impact methodology may not adequately capture the magnitude of all risk types. Atty. Fornier explained that expressing financial and operational risks in terms of their potential impact on company profits, net assets, or net value would be a valuable addition to the risk assessment process.

Mr. Martin agreed with Ms. Mantaring's suggestion and requested Atty.

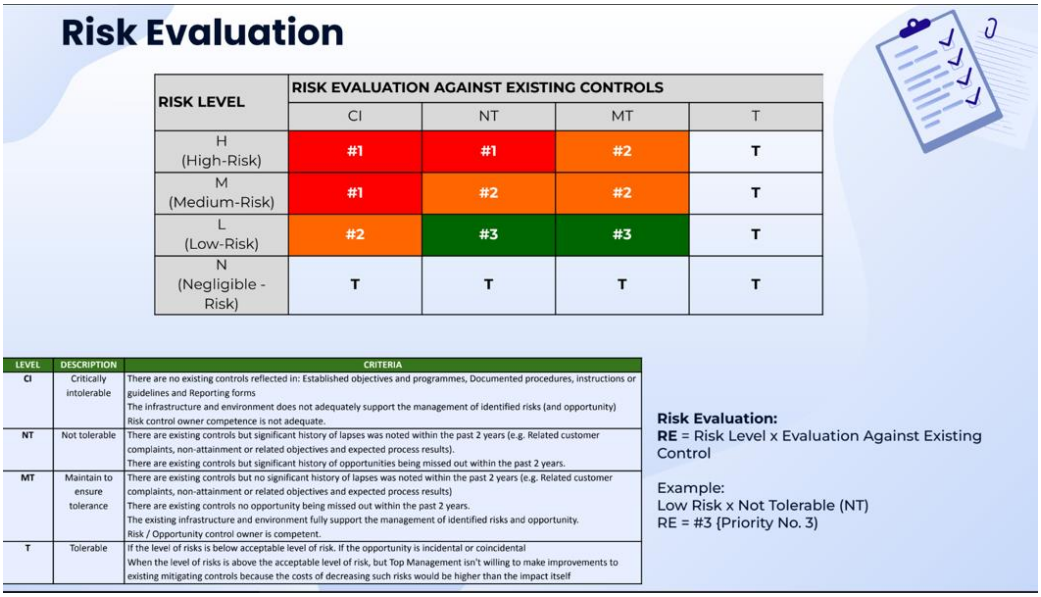
Fornier to add another parameter in the Heat Map table. Mr. Martin said that the likelihood consequence table and monetary consequence can be added.

Mr. Panganiban commented that adding monetary consequences was inevitable and it should be reconciled with the level of risk among enterprise-wide and departmental, division-wide, or business segment-wide risks. He illustrated that hypothetically, a building administration might consider a malfunctioning elevator in the Makati office as a very high risk. However, from an enterprise perspective, this incident might not be considered significant.

Thus, to effectively incorporate such department-level risks into the enterprise-wide risk assessment, assigning a monetary value to them is crucial. He also added that without a monetary value, it would be challenging to accurately aggregate and prioritize these risks within the overall enterprise risk report. Atty. Fornier agreed to add such parameters and he recognized that different categories of risk may have varying levels of financial appetite. Assigning peso values will enable a more accurate reflection of these varying tolerances. He explained that this approach was aligned with Mr. Panganiban's point that the significance of a particular risk can vary significantly between departments and individuals within the organization.

Mr. Rene J. Buenaventura ("**Mr. Buenaventura**") noted that based on his experience with two other companies (one regulated and one public), these companies have successfully implemented a threshold for the monetary value of risks. For example, a threshold of 2% of the company's top line could be established. Any risk with a calculated monetary value exceeding this threshold would be flagged for immediate attention and further investigation. Nonetheless, Mr. Buenaventura said that he agrees with adding a monetary value for each risk. Atty. Fornier then noted Mr. Buenaventura's suggestion and stated he would discuss it with the Senior Management Team ("**SMT**") to have a better appreciation and assessment of what level of financial impact constitutes dire consequences for the Corporation.

Next, Atty. Fornier presented the risk evaluation table:

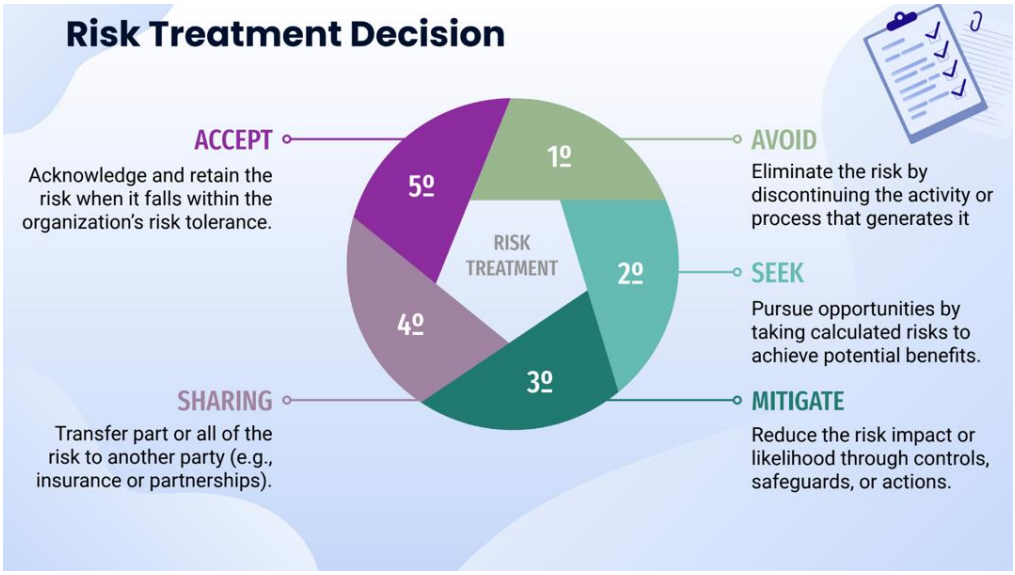


According to Atty. Fornier, this table reflected a proactive approach to risk management. He explained that it outlined a process where identified risks are evaluated against existing controls.

If a high-risk item is effectively mitigated through existing controls, its risk level is reduced to a tolerable level, and it is not considered a priority for risk management. Conversely, if a high-risk item is inadequately controlled or lacks sufficient controls, it is designated as a priority item for immediate attention.

The assessment of risk control effectiveness involves analyzing factors such as lapses, the number of errors, and the financial impact, including actual losses and potential penalties associated with the risk.

Atty. Fornier discussed that the diagram below showed the various risk treatment options adopted by the Corporation.



He discussed the various risk treatment options adopted by the Corporation:

- *Avoidance:* This involves completely eliminating the risk by discontinuing the activity or process that generates it. If an activity is deemed excessively risky or disruptive, regardless of potential opportunities, the Corporation may choose to avoid it entirely.

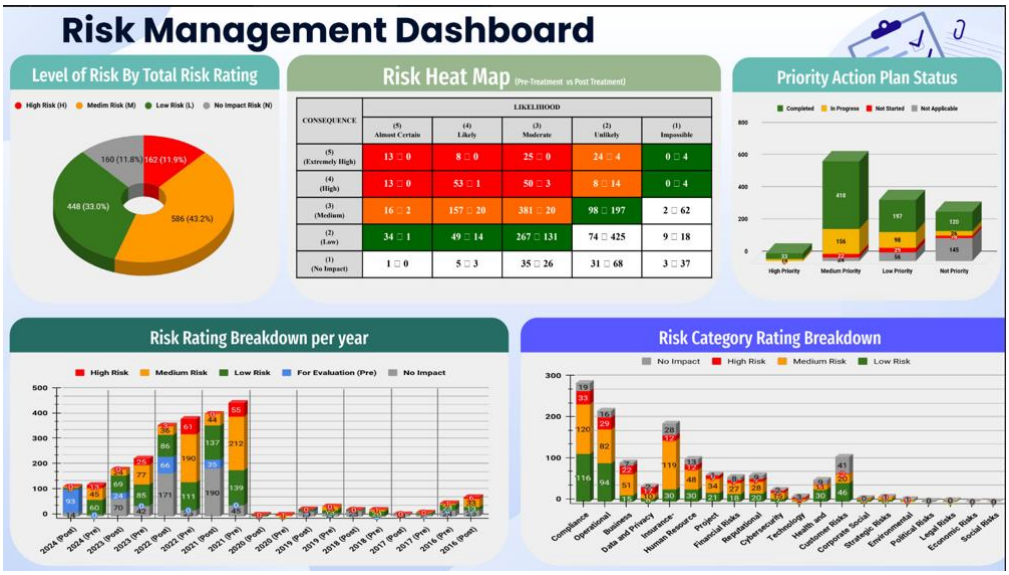
- *Seek Opportunity:* This more aggressive approach involves actively pursuing opportunities while acknowledging and managing associated risks.

- *Mitigation:* This is the most common risk treatment method, focusing on reducing the impact or likelihood of the risk through various actions, such as implementing controls, safeguards, and process improvements.

- *Sharing:* This involves transferring risk to a third party, such as through insurance. The company maintains cyber liability insurance to mitigate potential penalties or damages resulting from cyber incidents.

- *Acceptance:* This approach involves accepting the risk as part of the company's operations, provided it falls within the defined risk appetite or tolerance levels.

Atty. Fornier then presented a series of charts illustrating the evolution of identified risks since the inception of the risk framework in 2016. The charts focus on data from 2018 onwards, as the full framework and associated processes were implemented in that year.



He explained that the charts demonstrate a significant reduction in high-risk items over the past six years, attributed to the implementation of various treatments, actions, and policies across all departments. Each risk heat map displays two numbers: the initial number of risks identified at a particular level before treatment; and the number of risks remaining in that category after the implementation of risk treatment measures.

Mr. Panganiban inquired about the interpretation of the charts. He particularly asked the meaning of *thirteen (13)* in the Heat Risk Map above. Atty. Fornier said that the *thirteen (13)* is the number of risks at that level, which indicates an extremely high consequence and almost certain likelihood of occurring before the company treated them or before there were actions or policies in place to prevent, mitigate or avoid them.

Ms. Mantaring asked whether the second number (beside 13) was the residual risk. Atty. Fornier confirmed that it was the residual risk. Atty. Fornier explained that the first number was what it looked like prior to treatment and then post-treatment because of various actions, checks and balances, policies, and other similar means taken to minimize that certain risk. Thereafter, the risk was either reduced or eliminated, thus, it would fall later on into the green or white categories over time. He added that looking at the numbers, it can be observed that in the middle section, there are 381 risks that are of medium consequence and moderate likelihood then, these have been dropped to 20 as a result of the various actions taken by the Corporation over the years.

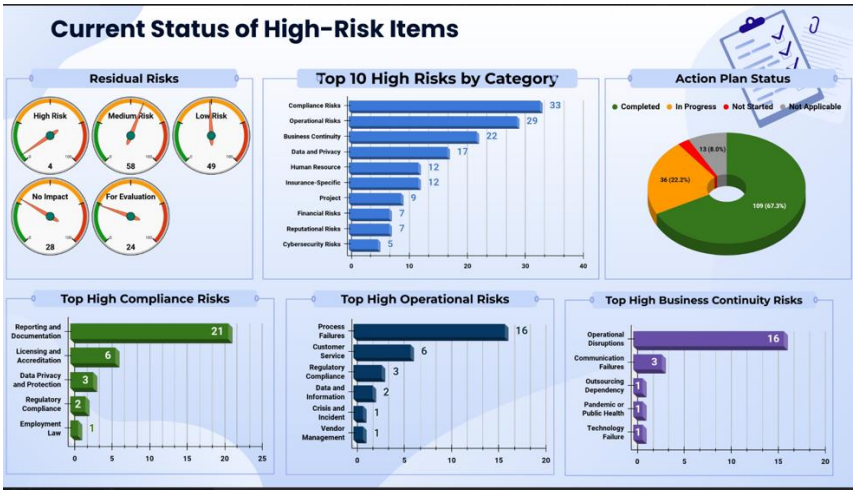
Mr. Panganiban asked for an example of these thirteen (13) items. Nonetheless, he noted that this was important to understand such instances considering that such risk was previously considered as “extremely high” and almost certain to happen but then had been categorized to zero risk.

In response, Atty. Fornier illustrated the data privacy risk or cyber liability would be an extremely high-risk event with high impact, high risk, high consequence, and high likelihood. If the company had completed treated it, then there’s no risk at all or perhaps not necessarily eliminated but dropped down to one of the lower risk categories. Ms. Mantaring added that the thirteen (13) to zero (0) do not necessarily mean that it was no longer a risk, it may have just moved down, either to orange level or yellow level.

Mr. Panganiban asked for the post-treatment chart of the heat map after all the risks have been down to zero. Ms. Mantaring also added that the risk map shows a voluminous number that may reflect the actual number of risks. She suggested to have a risk grouping and its corresponding position in the heat map. Mr. Panganiban elaborated that he would also like to see whether the top risks continue to remain in such category.

Mr. Christian S. Argos ("**Mr. Argos**") suggested that in the heat map, the risks categorized in red can be more detailed. Mr. Argos illustrated that the 13 risks that were both extremely high and almost certain have now been downgraded to either an orange, a green, or a white. He noted that it may be useful to add a complimentary presentation wherein all the red items are highlighted and should be addressed as per policy. This would properly communicate to the Committee which of the 13 would be in orange, green, or white. It might be a good investment in time to just focus on these risks and these could be perhaps grouped together.

Atty. Fornier then presented the following chart:



Ms. Mantaring requested on behalf of the Committee to provide a presentation focusing on residual risks rather than the initial risk levels. She explained that since mitigation efforts have already been implemented, the focus should be on the current risk levels after these mitigation efforts have taken effect. She emphasized that understanding the residual risk provides a more accurate and actionable picture of the current risk landscape, as the initial risk levels may not accurately reflect the current situation.

Atty. Fornier then presented the following table that may aid the Committee to see the current situation:

Sustained High Risks After Mitigation Efforts

Risk Category	Risk Item	Risk Statement	Core Process	Event	Probable cause	Decision	Action Plan	Target Completion Date	Status of Implementation	Remarks
Insurance -Specific Risks	Customer Experience and Service	Poor customer service or experience, leading to complaints, bad reviews, and potential loss of policyholders.	Franchising: Processing of franchise requests	Delayed processing of franchise approval	High volume of transactions	Mitigate Risk	Implement clear delegation of tasks among personnel for prioritization of focus areas	06/30/2022	Completed	Likelihood reduced from 4 to 3 after treatment, but impact remains at 4, requiring further attention.
Compliance Risks	Reporting and Documentation	Delayed submission of mandatory reports, risking non-compliance.	Partners Management Facilitation of annual agency performance review	Submission of incorrect and inaccurate performance review report	Incorrect report provided by Treasury Team/Database Team	Mitigate Risk	Validation of Sales Team to determine if agents included in the list have accounts under negotiation Use of naming convention	08/01/2022	Completed	No change observed; likelihood and impact remain at 3 and 4, respectively, indicating treatment has been ineffective. Further review is needed.
			Partners Management Facilitation of annual agency performance review	Submission of incorrect and inaccurate performance review report	Lack of attention to details	Mitigate Risk	Validation of Sales Team to determine if agents included in the list have accounts under negotiation Use of naming convention.	08/01/2022	Completed	No change observed; likelihood and impact remain at 3 and 4, respectively, indicating treatment has been ineffective. Further review is needed.
Insurance-Specific Risks	Network Provider Management	Risk of inadequate provider networks or failure to negotiate favorable reimbursement rates, resulting in poor member satisfaction.	Business Development. Grow the business across various segments	No or Limited accounts in areas without accredited providers.	- No or limited provider in the area - Unsuccessful accreditation of the PRO	Mitigate Risk	Continuous PCC expansion. Our team is looking for sites where they can set up a clinic. This is still an ongoing study to look for locations and to also review if we should build a mega clinic. We have expanded services of corporate clinics such as providing onsite phlebotomy and promotion of teleconsult and video consult.	12/31/2023	In Progress	Risk level upgraded due to increased impact (from 2 to 4) despite a reduction in likelihood (from 5 to 4), highlighting its importance. The target PCC was completed in 2023, with plans to expand further. The new target completion date needs to be updated.

High-Priority Mitigation Plans for High Risks

Risk Category	Risk Item	Risk Statement	Core Process	Event	Probable cause	Decision	Action Plan	Target Completion Date	Status of Implementation	Division / Remarks
Cybersecurity Risks	Third-Party Vendor Risks	Security vulnerabilities in third-party applications or service providers.	Cybersecurity	Unauthorized access to a third party application	Unauthorized access by compromising one user access.	Mitigate Risk	1. Enforce MFA across all systems either SSO or biometric authentication 2. Enforcing Dormant Policy on Third-Party Vendor Applications	10/31/2024	In Progress	Digital and Transformation *(June 2024 Data Breach)*
					Failed to ensure an adequate number of significant personnel in the information security department	Mitigate Risk	1. Implement regular training and awareness programs for management and staff on the importance of InfoSec. 2. Develop a proactive recruitment strategy for InfoSec personnel to avoid lapses in coverage.	10/31/2024	In Progress	Digital and Transformation *(June 2024 Data Breach)*
Operational Risks	Vendor Management Process Failures	Failure to assess vendor risk leading to operational vulnerabilities.	Vendor Performance	Not aware of existing government laws, rules and regulation	No cascade/advisory or orientation received	Mitigate Risk	Require the vendor to conduct training or orientation regarding the applicable government laws, rules and regulations	07/30/2024	In Progress	Health Network Management
		Inadequate monitoring of internal controls resulting in operational lapses.	SAP Development	integration Challenges	Data Synchronization Issues	Transfer Risk	With ongoing MIS Project c/o IT PMO	12/31/2025	In Progress	Finance and Treasury
			Hypercare	Functionality is not working as per user expectation	Incompiete scenarios to test full functionality and capture the defects	Mitigate Risk	Incident monitoring in production and root cause analysis	12/31/2025	In Progress	Finance and Treasury
Compliance Risks	Reporting and Documentation	Delayed, inaccurate, or insufficient submission of reports, risking non-compliance or disruption to business operations	Purchase Transaction	Double billing Delayed release of payment details	Delay on the release or lack of payment details Suppliers with Delayed Payments	Mitigate Risk	Integrate and evaluate a process analogous to JG, ensuring it is tailored to the unit's specific needs and operational context for optimal applicability and effectiveness.	07/30/2024	In Progress	Health Network Management

Note:
The action plan is still in progress, and its effectiveness will be evaluated once the implementation is complete.

Medium-Priority Mitigation Plans for High Risks

Risk Category	Risk Item	Risk Statement	Core Process	Event	Probable cause	Decision	Action Plan	Target Completion Date	Status of Implementation	Division / Remarks
Compliance Risks	Reporting and Documentation	Delayed, inaccurate, or insufficient submission of reports, risking non-compliance or disruption to business operations	Send Request for Pricing and Quotation	Delay in release of rate sheet	manpower and high volume of transactions for ACT, shortened deadline of client, dependency with operations for items needing quotations or approval	Mitigate Risk	To Ensure correctness in C4C - Request from ACT regarding Pricing Module update additional controls (C4C)	06/30/2025	In Progress	Corporate Sales
Data and Privacy Risks	Regulatory Non -Compliance	Failing to adhere to local, national, or international data protection laws governing patient data privacy.	Handling / processing of members personal information	Info security breach	Mishandling of data by Provider	Mitigate Risk	Request from DPO Team to Develop policy that will provide guidance in managing data breach caused by the provider Request from PRD to ensure providers have signed on the new contract	06/30/2025	In Progress	Corporate Sales
Customer Risks	Trust and Transparency	Risk of losing customer trust due to opaque pricing, unclear policies, or delayed claims processing.	Issuance of Quotation (not part of automated pricing)	Delay in release of quotation	Lack of Manpower	Mitigate Risk	Regular coordination with HRAD for continuous hiring; Internal Job postings and referrals	12/31/2024	In Progress	Actuarial
Business Continuity Risks	Operational Disruptions	Interruption of critical healthcare operations due to system failures or infrastructure breakdowns.	Migration to Cloud - Switching	Functionality of system is not working	Link of dependent systems are not updated to the target system	Mitigate Risk	Create a BCP for Cloud - AWS - SFDC	10/31/2024	In Progress	Digital and Transformation
				Software version of target system is not consistent with source system	Changes on-premise (source system) were not reflected on target system	Mitigate Risk	Install latest Kernel to target system Create a Migration Checklist (Google Form)	08/30/2024	In Progress	Digital and Transformation

Note:
The action plan is still in progress, and its effectiveness will be evaluated once the implementation is complete.

Mr. Martin explained that the Committee members were also interested in the high risks that have been originally identified and which mitigation strategies were provided for thus resulting to a lower residual risk, which might still be in the medium category as well and not just sustained or those where mitigation strategies were provided for and which resulted in lower residual, but still presents a certain degree of risk to the Corporation. He further suggested to present a worksheet detailing these and a more granular presentation.

Mr. Panganiban stated that the table illustrates the difficulty in determining which are the high-level risks. For instance, the insurance risk category includes "customer experience and service" as a risk item. While this risk has been mitigated to a certain extent, with the likelihood reduced from four to three after treatment, the specific impact remains unclear.

In line with that he clarified when it was considered as 'customer experience and service' and whether this refers to half of Maxicare's customers, or was

it one-third, or perhaps only five or six who complained. Mr. Panganiban emphasized that the presence of any complaint, regardless of the scale, suggests that the risk had not been fully mitigated.

This lack of specificity in the data, Mr. Panganiban posits, can lead to misinterpretations. Without quantifying the impact, such as by assigning a monetary value or measuring the percentage of affected customers, it becomes difficult to accurately assess the true significance of the risk. For example, even if 100 customers complained, the impact might be negligible if the company serves millions of customers.

Atty. Fornier responded that a rating of 3 or 4 represents between 5% and less than 10% of the total membership and this likely reflects the intended scope of "poor customer service." Therefore, Atty. Fornier clarified that "poor customer service" likely refers to a broader issue affecting between 5% and 10% percent of the total membership, rather than isolated incidents involving a small number of individuals. He explained that this level of impact, affecting a significant portion of the membership, warrants continued attention and mitigation efforts as it poses a significant risk to the business and its reputation.

Mr. Martin clarified Mr. Panganiban's concern that the details of the 10% were not immediately evident from the table provided. Atty. Fornier said that the points raised by the Committee will be carefully considered for the next iteration of the report. While this presentation primarily aimed to illustrate the current state of the Corporation’s risk management setup, it is clear that improvements, particularly in reporting, are necessary. The next version will focus on enhancing the specificity and clarity of certain areas.

Atty. Fornier continued with the discussion of the tables presented. He showed that the following sustained high-risk status even after mitigation: customer experience, compliance and reporting, submission of reports, and network provider management.

High-Priority Mitigation Plans for High Risks

Risk Category	Risk Item	Risk Statement	Core Process	Event	Probable cause	Decision	Action Plan	Target Completion Date	Status of Implementation	Division / Remarks
Cybersecurity Risks	Third-Party Vendor Risks	Security vulnerabilities in third-party applications or service providers.	Cybersecurity	Unauthorized access to a third party application	Unauthorized access by compromising one user access.	Mitigate Risk	1. Enforce MFA across all systems either SSO or biometric authentication 2. Enforcing Dormant Policy on Third-Party Vendor Applications	10/31/2024	In Progress	Digital and Transformation *(June 2024 Data Breach)*
					Failed to ensure an adequate number of significant personnel in the information security department	Mitigate Risk	1. Implement regular training and awareness programs for management and staff on the importance of InfoSec. 2. Develop a proactive recruitment strategy for InfoSec personnel to avoid lapses in coverage.	10/31/2024	In Progress	Digital and Transformation *(June 2024 Data Breach)*
Operational Risks	Vendor Management Process Failures	Failure to assess vendor risk leading to operational vulnerabilities.	Vendor Performance	Not aware of existing government laws, rules and regulation	No cascade/advisory or orientation received	Mitigate Risk	Require the vendor to conduct training or orientation regarding the applicable government laws, rules and regulations	07/30/2024	In Progress	Health Network Management
		Inadequate monitoring of internal controls resulting in operational lapses.	SAP Development	Integration Challenges	Data Synchronization Issues	Transfer Risk	With ongoing MIS Project c/o IT PMO	12/31/2025	In Progress	Finance and Treasury
			Hypercare	Functionality is not working as per user expectation	Incomplete scenarios to test full functionality and capture the defects	Mitigate Risk	Incident monitoring in production and root cause analysis	12/31/2025	In Progress	Finance and Treasury
Compliance Risks	Reporting and Documentation	Delayed, inaccurate, or insufficient submission of reports, risking non-compliance or disruption to business operations	Purchase Transaction	Double billing Delayed release of payment details	Delay on the release or lack of payment details Suppliers with Delayed Payments	Mitigate Risk	Integrate and evaluate a process analogous to JG, ensuring it is tailored to the unit's specific needs and operational context for optimal applicability and effectiveness.	07/30/2024	In Progress	Health Network Management

Note:
The action plan is still in progress, and its effectiveness will be evaluated once the implementation is complete.

Meanwhile, the high priority mitigation plans for high risk refer to the cybersecurity risks. The team would go into the fine details of the Corporation's information security and cybersecurity setup. He explained that there were certain steps that need to be taken or that have been taken but were still in progress.

As to the June 2024 data breach situation wherein one of Maxicare's service providers experienced a hacking by a third-party perpetrator, Maxicare was compelled by circumstances to address that breach directly, even though it was technically not its responsibility. He discussed that even the vetting of third-party vendors and their infrastructure for cybersecurity is a risk that must be managed. Under the operational risk, there is a need to assess vendor operational vulnerabilities as well as their own compliance.

Mr. Buenaventura asked Mr. Argos whether it was Maxicare that was held accountable for the aforementioned data breach in June 2024. Mr. Buenaventura clarified whether Maxicare was the one accountable for this data breach in June 2024.

Mr. Argos confirmed that it was not Maxicare. He explained that eventually it was identified that it was the third-party partner since it was their system that was hacked. Despite that, the person who was technically attacked was Maxicare's employee, the third-party service provider should have included a two-factor authentication system and even some controls on the server side or on the system side. It had been identified that thousands of records were being accessed within milliseconds of each other doing a query. These are things that Maxicare could not implement because Maxicare was not

the owner of the platform. It was also determined that the third- party was the personal information controller ("**PIC**") for that matter.

Mr. Buenaventura asked the status of this with the National Privacy Commission ("**NPC**"). Mr. Argos said that there have been joint sessions with the NPC but there was still no final report on the matter. Atty. Fornier said that based on his resource personnel, it would take some time before NPC issues a final report considering their low manpower vis-à-vis the number of complaints they have been receiving. Atty. Fornier then noted that the SMT has been very cooperative with NPC and that the NPC had interviewed some of the team members.

Mr. Buenaventura said that they could discuss the recent developments of the data breach case in a different forum. Mr. Argos said that this had been a long tail of the process to officially close out the case. But in the course of the investigation, the SMT invited the PIC to participate and the NPC had direct engagement already with the third-party provider as the PIC.

Ms. Mantaring suggested that when an incident such as a data breach happens, there should be a notification to the Committee. She said that she only found out about the said breach through the public and the news. This is to aid and apprise the Committee should they be interviewed or asked about the incident. Atty. Fornier emphasized the importance of regular meetings with directors to facilitate the exchange of information and ensure timely updates. He highlighted that in the event of significant incidents, appropriate reports will be provided to the Board of Directors and the Committee for their information and potential action.

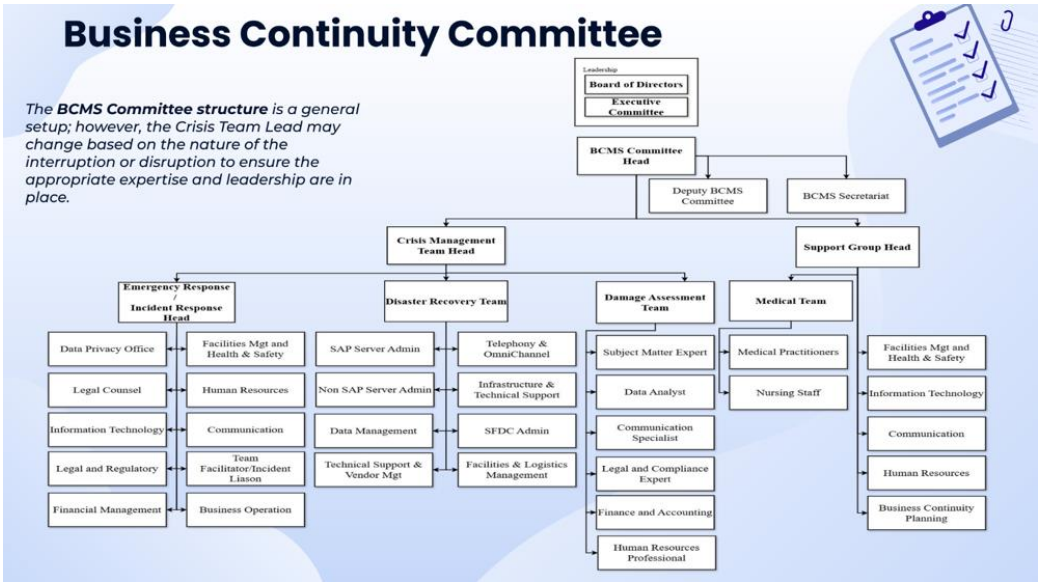
Mr. Buenaventura noted that there was a script provided in answering external inquiries. He suggested that this script should be shared to the Board of Directors. Mr. Panganiban said that this should be included in the Crisis Committee process or in the business continuity manual. In response to Mr. Enrico S. Cruz ("**Mr. Cruz**") query, Atty. Fornier confirmed that this was part of the Incident Management Manual. He added that communication was one of the key elements of management of data breach crises, hence, it was part of the standard operating procedure.

Mr. Argos also discussed that there was a session last month with the JG Corporate Affairs and Crisis Management Team in a specific workshop to strengthen Maxicare's policy for crisis management. Determining the pre-work to be done and linking it to Maxicare's risk register for those that are likely or the more likely in high impact risk. The team is developing these standardized standard processes that would allow business continuity and

crisis management. He noted that stakeholder management was a key topic of the workshop along with external communications. The action item from that workshop was to create a crisis management plan for identified key risks.

V. BUSINESS CONTINUITY PLAN

Atty. Fornier then proceeded to report on the Business Continuity Plans ("**BCP**") for Critical Areas. He presented the current business continuity committee of the Corporation:



Atty. Fornier discussed that in the event that a crisis arises, this is the table or the tree of individuals or departments that Maxicare would pull from for the assessment, management, and resolution of any crisis under business continuity. The number of individuals involved in the departments that would take charge would vary depending on the type of crisis. He explained that this was at least the all-encompassing general framework of who Maxicare would rely on in the event of a crisis from the Business Continuity Committee Head to an actual Crisis Management Team Head who would be pulled from various teams. He noted that seemingly it was more skewed towards natural or physical disasters, but he explained that this was also a work in progress.

Atty. Fornier also recognized that this diagram could be shrunk down, making it more responsive to certain types of risks. It could be broken down to identify only those individuals who are critical or who are specifically relevant to that particular type of risk or type of crisis.

Mr. Martin asked whether each individual understood their respective responsibility when a crisis occurs. Atty. Fornier negated that statement and said that in the current state of things, the individuals were not yet vetted for their respective responsibilities. The diagram was merely a picture of the Crisis Committee for top management to understand when a crisis occurs and who they would have to pull in. Thus, Mr. Martin suggested that the next step is to make the individuals understand the existence of the Business Continuity Committee and the existence of the Crisis Committee and their respective roles in those committees.

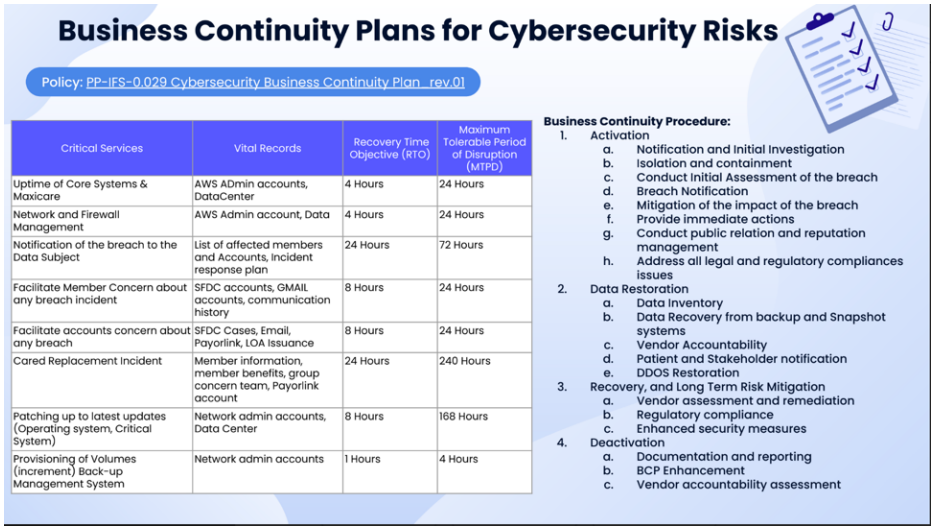
In addition to Mr. Martin's point, Mr. Panganiban recommended that the individuals should maintain a readily accessible emergency contact list or call tree. This list, containing key contact numbers, should be kept in a small, portable format such as an index card or a piece of paper that can be stored in a wallet. Mr. Panganiban emphasized the importance of this practice, noting that in a crisis situation, individuals may not have access to their usual resources, such as office manuals or home directories. Having a readily available emergency contact list can help individuals quickly connect with necessary personnel and respond effectively to the situation.

Atty. Fornier agreed with Mr. Panganiban's suggestion and furthered that a digital iteration of such can be done, probably through a mobile application.

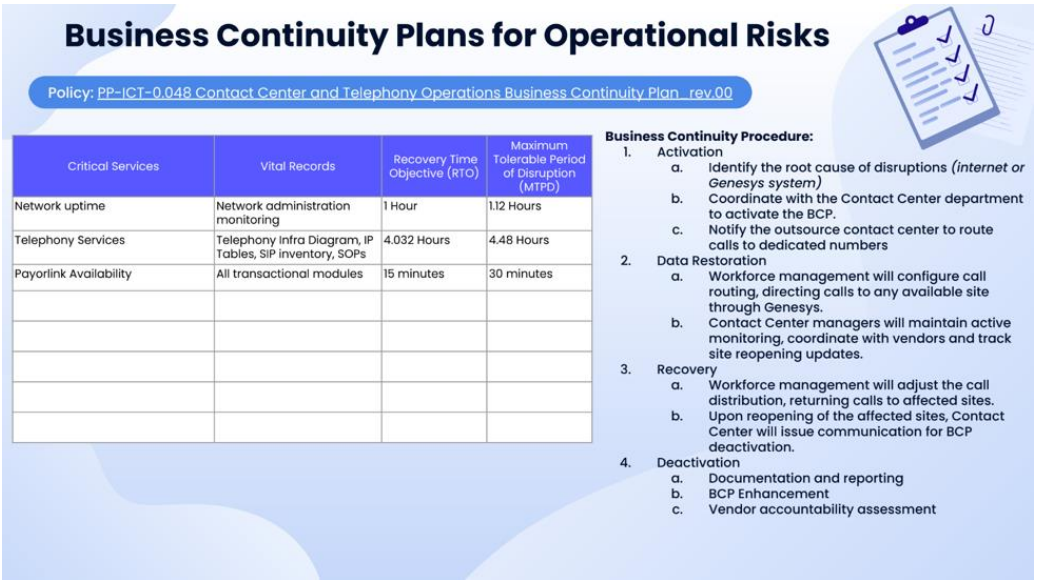
Ms. Mantaring reminded the Committee that there can be instances wherein there is no cellular signal. Thus, she suggested that alternative methods should be thought out and prepared for these kinds of situations. In response to Mr. Martin's query, Atty. Fornier confirmed that Maxicare has a call tree, which was effective during typhoons. Mr. Martin also suggested that the call tree response time should be tested. Ms. Mantaring suggested that the number of responses should be recorded and their response time to check whether the call tree is working.

Atty. Fornier confirmed that there was a call tree documented in the Google Sheet that was available to everyone in the Corporation. He agreed that the testing of that call tree's effectiveness iwas a necessary exercise.

Atty. Fornier then expounded on the BCP for the cybersecurity risks, operational risks, and operational disruptions. He presented the matrix relative to this:

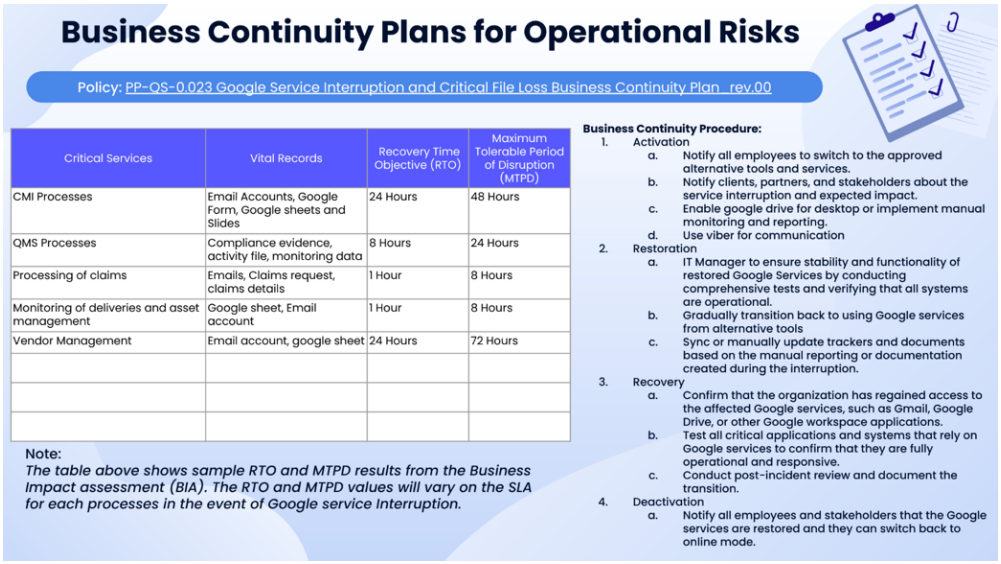


Atty. Fornier then presented the BCP for operational risks:



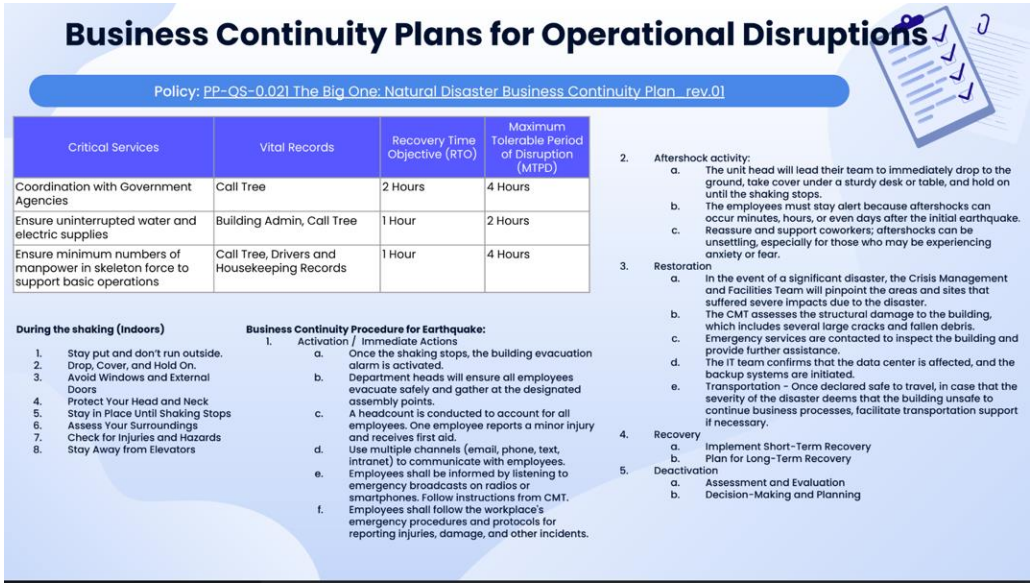
He discussed that under these are the contact center and telephone operations.

He also presented the BCP for service interruption:



He discussed that Maxicare is under the Google service suite, and in case of interruption and critical file loss, these were the metrics that had been adopted and the steps for the procedure.

Atty. Fornier then presented the BCP for natural disasters, particularly “the big one” (earthquake).



The presentation outlined the steps to be taken in the event of an earthquake. While detailed BCPs exist for various major crises, the company recognizes the ongoing need for continuous improvement and the potential for unforeseen crises. Efforts to identify and address these potential gaps will continue.

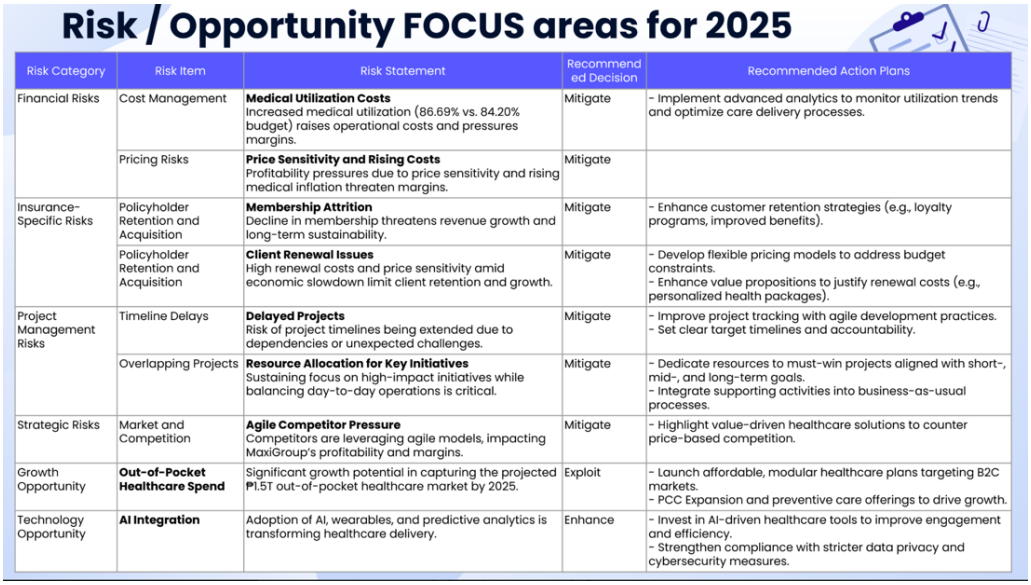
Mr. Martin asked whether the IT department was aware of the Recovery Time Objectives ("RTO"). Atty. Fornier explained that the BCP was developed in collaboration with the IT Department and other relevant departments. This collaborative process ensured that all departments were aware of and involved in the policy development. Further, the key performance indicators ("KPI") outlined in the policy serve as guidelines for departments when working with third-party providers or developing their infrastructure. These KPIs establish specific standards that must be met in all relevant operational areas.

Mr. Martin then emphasized the importance of establishing Recovery Point Objectives ("RPO") in addition to RTO. While RTOs define the acceptable time frame for restoring service after an outage, RPOs focus on the acceptable data loss that can occur during an outage. Mr. Martin explained that even if an application can be restored quickly (e.g., within two hours), significant data loss can severely impact a department's ability to function effectively. Therefore, departments must define their RPOs, specifying the maximum acceptable data loss in terms of time (e.g., one hour, one day, one week). This ensures that data recovery aligns with the specific business needs and minimizes disruption to operations.

Atty. Fornier took Mr. Martin's suggestion into advisement. He acknowledged that while RPOs may not be explicitly stated in the current policy, these are considered an important aspect of business continuity planning. Atty. Fornier confirmed that RPOs will be explicitly included in the next update of the BCP.

It was suggested by Mr. Panganiban that in future Committee meetings, there should be a dedicated portion to have a detailed discussion of the IT recovery process. This discussion would cover crucial aspects such as backup strategies, including offsite backups, to ensure a comprehensive understanding of the critical role IT plays in business continuity. Mr. Martin agreed with Mr. Panganiban, and he suggested that the discussion on risk mitigation should specifically address the impact of application, system, or data center outages. This would involve examining the specific protections in place to mitigate the risks associated with such disruptions.

The following presentation outlined several risk and opportunity focus areas identified based on the 2025 strategic plan.



Risk / Opportunity FOCUS areas for 2025

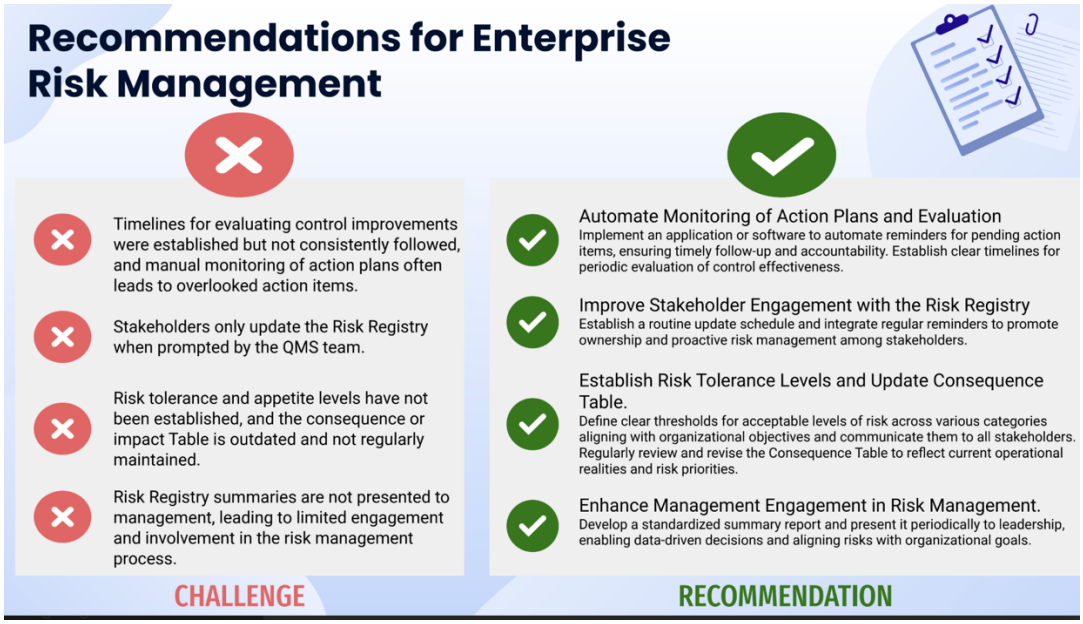
Risk Category	Risk Item	Risk Statement	Recommended Decision	Recommended Action Plans
Financial Risks	Cost Management	**Medical Utilization Costs** Increased medical utilization (86.69% vs. 84.20% budget) raises operational costs and pressures margins.	Mitigate	- Implement advanced analytics to monitor utilization trends and optimize care delivery processes.
	Pricing Risks	**Price Sensitivity and Rising Costs** Profitability pressures due to price sensitivity and rising medical inflation threaten margins.	Mitigate	
Insurance-Specific Risks	Policyholder Retention and Acquisition	**Membership Attrition** Decline in membership threatens revenue growth and long-term sustainability.	Mitigate	- Enhance customer retention strategies (e.g., loyalty programs, improved benefits).
	Policyholder Retention and Acquisition	**Client Renewal Issues** High renewal costs and price sensitivity amid economic slowdown limit client retention and growth.	Mitigate	- Develop flexible pricing models to address budget constraints. - Enhance value propositions to justify renewal costs (e.g., personalized health packages).
Project Management Risks	Timeline Delays	**Delayed Projects** Risk of project timelines being extended due to dependencies or unexpected challenges.	Mitigate	- Improve project tracking with agile development practices. - Set clear target timelines and accountability.
	Overlapping Projects	**Resource Allocation for Key Initiatives** Sustaining focus on high-impact initiatives while balancing day-to-day operations is critical.	Mitigate	- Dedicate resources to must-win projects aligned with short-, mid-, and long-term goals. - Integrate supporting activities into business-as-usual processes.
Strategic Risks	Market and Competition	**Agile Competitor Pressure** Competitors are leveraging agile models, impacting MaxiGroup's profitability and margins.	Mitigate	- Highlight value-driven healthcare solutions to counter price-based competition.
Growth Opportunity	**Out-of-Pocket Healthcare Spend**	Significant growth potential in capturing the projected ₱1.5T out-of-pocket healthcare market by 2025.	Exploit	- Launch affordable, modular healthcare plans targeting B2C markets. - PCC Expansion and preventive care offerings to drive growth.
Technology Opportunity	**AI Integration**	Adoption of AI, wearables, and predictive analytics is transforming healthcare delivery.	Enhance	- Invest in AI-driven healthcare tools to improve engagement and efficiency. - Strengthen compliance with stricter data privacy and cybersecurity measures.

Atty. Fornier discussed the organic nature of the ERM and its crucial role in supporting company strategy. These focus areas were identified proactively rather than solely in response to specific incidents. These focus areas likewise include emerging risks such as the potential benefits and risks associated with Artificial Intelligence ("AI"), the increasing significance of medical utilization management given tighter financial constraints, and heightened price sensitivity. He then discussed the competitive risk emphasized by the legal counsel of the JG Team. He mentioned that this was also included as a key focus area due to its significant impact on the business. Other identified focus areas include client renewal, membership attrition, and project delays.

Atty. Fornier also discussed the recommended action plans for these focus areas, which are currently in their initial stages and were developed through internal brainstorming sessions. These plans will undergo further refinement through collaboration and discussions with relevant departments and subject matter experts. The overarching goal is to ensure that risk management is fully integrated with the Corporation's strategic focus and approach, moving away from a purely reactive approach.

VI. RECOMMENDATIONS FOR THE ERM

Atty. Fornier presented some challenges of the QMS team and risk management had faced over the last five to six years.



These challenges included:

- *Delays in evaluating control improvements:* Timelines for evaluating the effectiveness of control improvements were often not adhered to.

- *Inconsistent risk registry updates:* Risk registries were frequently updated only when risks reached critical levels, exceeding established tolerances and appetites.

- *Limited visibility of risk management activities:* The visibility of risk registry summaries, the risk management framework, and the outcomes of opportunity and risk assessments were insufficient, particularly among senior management and the board of directors.

To address these challenges, the team plans to implement several key improvements, which include the following:

- *Automation of risk management processes*: Automating certain aspects of risk management will enhance efficiency, improve buy-in, and increase awareness of the importance of risk management across all departments.

- *Establishment of clear risk tolerance levels*: Defining and implementing clear risk tolerance levels, including the monetary value of potential impacts, will enable more accurate risk assessment and prioritization.

- *Enhanced management engagement:* Increased engagement from all levels of management, including division heads, will be crucial. This will foster a greater understanding of the value of risk management and ensure that it is viewed as an integral part of the decision-making process across all departments.

By addressing these challenges and implementing these improvements, the Corporation aims to strengthen its risk management function and ensure that it effectively supports the overall business objectives.

Mr. Panganiban expressed his concern about the list presented, especially with the third bullet under "X" or risk tolerance and appetite levels that have not been established, and the consequence of the impact table is outdated and not regularly maintained. He asked whether the SMT and even the Board of Directors have not yet approved Maxicare's risk appetite for certain areas of the business.

Atty. Fornier responded that there was a need for a more clearly defined framework for acceptable and unacceptable risk levels. While some parameters may exist based on past experiences and informal discussions, a more formal framework, such as a table of standards or a clearly defined set of criteria, is necessary to ensure consistent and objective risk assessments.

Mr. Panganiban highlighted the importance of clearly defined risk appetite levels to maintain discipline within the organization. Without established risk appetite levels, aggressive business managers may pursue higher-risk ventures that exceed the organization's tolerance, potentially leading to negative consequences. He emphasized that clearly defined risk appetite levels are crucial for creating an environment where all stakeholders, including business managers, understand the acceptable boundaries for risk-taking and are held accountable for adhering to those boundaries.

Atty. Fornier acknowledged Mr. Panganiban's concern regarding potential over-aggressiveness in risk-taking. However, Atty. Fornier observed that the current risk management approach within the organization tends to be overly conservative, potentially hindering the pursuit of valuable opportunities and limiting the organization's agility and adaptability compared to competitors. He emphasized the importance of establishing clear risk tolerance levels while the organization operates within a relatively conservative framework. This proactive approach will provide a structured framework for gradually increasing risk appetite and encouraging innovation while mitigating the potential for excessive risk-taking.

Atty. Fornier highlighted that the risk management program itself can serve as a valuable tool for guiding this controlled expansion of risk appetite, enabling the organization to explore new opportunities while maintaining a responsible and measured approach.

Mr. Martin expressed his assumption that the business has established limits in terms of what they can and cannot do. Atty. Fornier opined that it was organic on how the business was being conducted. Atty. Fornier suggested that while existing policy and process controls, along with checks and balances, provide a foundation for risk management, the current framework could be enhanced by establishing more specific and quantifiable parameters for acceptable risk levels.

Mr. Martin asked whether there were certain limits for even transactional limits where, at a certain point, the next higher level of authority needs to get involved. Mr. Argos confirmed that Maxicare has certain limits. He explained that this was determined both at the management level and at certain amounts, it goes up to the shareholder level. He discussed that at the highest threshold, at the disbursement side, Maxicare requires two Class A signatories, and we have Class A1 and Class A2 belonging to the two shareholder groups.

Mr. Argos noted that existing policies govern the budgeting process. The company's annual budget, including operating expenses ("OPEX") and capital expenditures ("CAPEX"), was approved by the Executive Committee ("EXCOMM") in November of the previous year. Supporting documentation for the approved budget was provided as part of the presentation. Mr. Argos also mentioned that policies are in place regarding contract signing, including guidelines on the nature and scope of contracts.

In conclusion, Atty. Fornier expressed gratitude for the opportunity to present the current state of the risk management framework. He acknowledged that while the framework is operational and actively maintained, there was always room for improvement, both in terms of reporting and the overall framework itself. Atty. Fornier emphasized that the team was committed to ongoing refinement of the risk management framework, particularly incorporating the valuable suggestions and feedback received during the meeting.

Mr. Martin inquired about the nature of the risk-monitoring process. He specifically asked whether the company maintains a fixed set of monitored risks or if the risk register was dynamically updated annually. Mr. Martin sought clarification on whether the risk identification process involved

regular interviews with business units to identify emerging and new risks, which are then incorporated into the updated risk register.

Atty. Fornier explained that the risk analysis and infrastructure are defined through an annual workshop process that spans several months. This process involves extensive discussions with various stakeholders. He clarified that while some risks may remain relevant from year to year, the workshop also focuses on identifying and incorporating emerging risks that may be specific to each division. These discussions ensure that the risk register remains dynamic and reflects the evolving risk landscape within the organization.

Mr. Martin also asked about the ongoing management of the risk register. He specifically asked whether the register was expected to grow continuously or if there was a process for removing risks that have been fully addressed or mitigated. Mr. Martin also sought clarification on the mechanisms used to maintain and update the risk register on an ongoing basis. Atty. Fornier explained that the risk register was subject to ongoing review and maintenance. Risks that have been fully mitigated, or those with negligible likelihood and impact, are typically removed from the register to prevent clutter and ensure that the focus remains on the most critical risks. This process helps maintain the clarity and focus of the risk register.

Mr. Argos informed the committee that the SMT identified additional risks and opportunities that will require the development of specific action plans for 2025. These identified risks and opportunities will be incorporated into the risk register throughout the year.

Mr. Argos highlighted that the presentation by Atty. Fornier revealed that the QMS Team had been actively working on risk management initiatives, particularly in the context of ISO certification and accreditation. This existing body of work, while valuable, had not been adequately socialized at the committee level or integrated with the audit function and the newly created risk function within Maxicare.

Mr. Argos explained that recent organizational changes, including the placement of Ms. Gladice Censon ("Ms. Censon") and her team under Atty. Fornier's leadership had facilitated the integration of these existing efforts. This integration aims to leverage the existing body of work while aligning it with the terminology, methodology, and best practices adopted by the JG Team.

He expressed optimism, noting that while the initial assessment suggested a significant gap in existing risk management efforts, the team discovered a

valuable foundation of work already undertaken by Ms. Censon and the QMS Team. This foundation has enabled the team to accelerate the risk management process by leveraging existing resources. Mr. Argos emphasized that ongoing efforts are necessary to fully integrate the existing practices with the new framework and ensure a smooth transition.

Mr. Panganiban emphasized the importance of socializing the existing body of risk management work, ensuring that all stakeholders understand its purpose and adhere to the established risk appetite parameters. He acknowledged that reviewing the entire risk register in detail during each committee meeting would be impractical. Therefore, Mr. Panganiban suggested that each meeting dedicate time to review the top 10 risks. Mr. Panganiban explained that while the ranking of these top risks may change over time due to mitigation efforts or emerging risks, this regular review will ensure that the committee remains informed about the most critical risks facing the organization and can make informed decisions accordingly.

Mr. Martin and Mr. Argos requested that Atty. Fornier send a copy of the legal and risk compliance organizational chart (the entire body) with the individuals and their roles. Atty. Fornier noted the request. He also noted that while the risk management function has dedicated individuals, other departments, such as compliance, data privacy, and legal, also play a crucial role in risk identification and mitigation. He suggested that it would be beneficial for the committee to have a comprehensive overview of the risk management activities undertaken by these various departments to gain a holistic understanding of the organization's overall risk profile.

VII. ADJOURNMENT

There being no other matters discussed and upon motion duly seconded, the meeting was adjourned.

CERTIFIED TRUE AND CORRECT:

ATTY. DANNY E. BUNYI
Corporate Secretary

ATTESTED BY:

RICARDO V. MARTIN
Chairperson

ENRICO S. CRUZ

RIZALINA MANTARING

TEODORO M. PANGANIBAN

ANNEX A
Matters Arising from the 20 December BROC Meeting

A. *Heat Map – Monetary Value*

A detailed narration of assigning monetary values to certain risk categories in the heat map is indicated in the succeeding of sections this Minutes. Among the suggestions was to add values in the various risk categories. It was also proposed that thresholds be incorporated for every level of risk. A post-treatment chart of the heat map was likewise requested after all the indicated risks have been down to zero.

B. *Specific Examples of the High-Level Risk*

Specific examples of the high-level of risk were asked by the Committee, which the Legal and Risk Compliance deferred to the head of the Quality Management System.

C. *Reporting of the Risk Items and Risk Dashboard*

It was noted that the actual number of risks as reflected in the risk map were voluminous. To address this, risk grouping was suggested.

D. *Incident Notification*

It was proposed that the Committee and the Board of Directors be given a notification in case there are high-level risks or incidents of high public interest (i.e. data breach) in order to apprise the Committee and the Board of the incident. There was also a suggestion to provide the Committee and the Board of Directors with the scrip to answer any external inquiries.

E. *Detailed Report on the High-Level Risk*

It was proposed that a discussion of the top risks be provided alongside the heat map. A focused discussion of the red items and how it should be addressed based on company policy must likewise be made. Additionally, it was suggested that the top 10 risks be reported in every meeting.

F. *Residual Risk Report*

It was proposed that a post-treatment risk report should be done. The Committee requested a presentation that focuses on residual risks rather than the initial risk levels. This shift in focus would provide a more accurate and actionable understanding of the current risk landscape, as mitigation efforts may have significantly altered the initial risk levels.

This proposal also emphasized the importance of understanding the current risk profile after considering the impact of implemented mitigation strategies. A worksheet detailing former high risks which have been decreased to lower residual risks due to mitigation strategies was requested.

G. Report on the Recovery Point of Objective of IT

First, it was proposed that in a future meeting, a portion be dedicated to a detailed discussion of the IT recovery process, covering crucial aspects such as backup strategies, including offsite backups, to ensure a comprehensive understanding of the critical role IT plays in business continuity. Second, the Committee proposed that the discussion on risk mitigation should address the impact of application, system, or data center outages, examining the specific protections in place to mitigate the risks associated with such disruptions. These proposals aim to enhance the Committee's understanding of critical IT recovery processes and the specific mitigation strategies to address potential disruptions. Third, it was noted that even if an application can be restored quickly (e.g., within two hours), significant data loss can severely impact a department's ability to function effectively. As such departments must define their RPOs, specifying the maximum data loss in terms of time (e.g., one hour, one day, one week). This ensures that data recovery aligns with business needs and minimizes disruption to operations.

H. Call Tree Testing

The Committee proposed two measures to enhance the effectiveness of the emergency contact list. First, it was suggested that regular tests be conducted to evaluate the response times of the emergency contact list. Second, the Committee recommended recording the number of responses received during each test and their corresponding response times to track the overall effectiveness of the emergency contact list. These proposals aim to ensure the timely and effective activation of emergency response procedures.

I. Crisis Management Team and Business Continuity Team

The Committee suggested that the next step in enhancing business continuity awareness was to educate all employees on the existence and roles of the Business Continuity Committee and the Crisis Committee. This proposal aimed to increase employee awareness of the available resources and support systems in the event of a crisis.