MAXICARE HEALTHCARE CORPORATION

MINUTES OF THE MEETING OF THE BOARD RISK OVERSIGHT COMMITTEE[1]

Boardroom, Maxicare Tower
203 Salcedo Street, Legaspi Village, Makati City[2]
13 August 2024, 10:00 A.M.

PRESENT:

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

ALSO PRESENT:

ROBERTO P. ANG
RENE J. BUENAVENTURA
BRIAN M. GO
CHRISTIAN S. ARGOS
JASPER HENDRIK T. CHENG
JOSEPH JAY MAURICIO
ROSELLE RIVERA
JERRY PEREZ
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 jointly with the Chairperson of the Audit Committee, Mr. Teodoro M. Panganiban, ("**Mr. Panganiban**"). 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

[1] The meeting was conducted jointly with the Audit Committee and its advisers.
[2] 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.

"**Corporation**", "**Maxicare**", or "**MHC**") By-Laws and he certified the existence of a quorum for the transaction of business at hand.

II. MATTERS ARISING FROM THE MINUTES

The following items arose from this inaugural Committee meeting:

A. *Approval of the Committee Charter:*

As subsequently narrated in these minutes, the Committee Charter was presented to the committee members. This was subsequently approved for endorsement to the Corporation's Board of Directors by the members subject to some revisions to be made in the draft presented.

The Committee Charter was presented to the Board of Directors in its 25 October 2024 meeting and was duly approved.

B. *Contractual Remedies to be Incorporated in Maxicare's Agreements with Third-Party Providers in Relation to Events of Data Breach:*

It was discussed that contracts with third-party providers must be enhanced to include remedies in the event of data breach, especially when the Corporation or its members are impacted by providers who are the personal information controller.

C. *Risk Management Strategy:*

A detailed narration of the proposed Risk Management Strategy is indicated in the succeeding sections. Among the suggestions in this area were to have a set of acceptable minimum standards which can be used to cross-reference all Maxicare's counterparties and vendors in terms of cybersecurity and IT security. This would standardize procedures for handling future data breach situations. Conducting trainings on crisis management and business continuity principles was also proposed.

D. *Formation of Maxicare Crisis Management Team:*

A proposal to form a Maxicare Crisis Management Team was brought up, which would be responsible for swiftly responding to data breach incidents, actively engaging with the media, and proactively shaping the public narrative to minimize reputational damage.

E. *Risk Criteria:*

In the presentation of the risk appetite of the Corporation, it was proposed that MHC's risk criteria must be identified. A risk sliding scale would also be reported.

It was likewise discussed that a detailed plan must be presented for formalizing the Corporation's Enterprise Risk Management system. The types of risk covered (i.e. credit, liquidity, interest rate, reputational, information security, and operations) must also be tackled.

III. BOARD RISK OVERSIGHT COMMITTEE CHARTER

This is the first Committee meeting and Mr. Martin initiated the discussion by inviting Atty. Andrew Fornier ("**Atty. Fornier**") to proceed with his presentation by going through the major items in the Committee Charter (the "**Charter**"), which was distributed to the Committee members prior to the meeting. He explained that the Charter contained the composition of the Committee, meeting frequency, duties of the Committee, and Committee members. Regarding the frequency of the meeting, it was set to be done quarterly, subject to the approval of the Committee should they wish to have meetings more frequently.

Atty. Fornier explained that the risk management strategies of the Corporation would be primarily handled by the Senior Management Team ("**SMT**") and the responsible personnel of MHC. He then discussed the risk oversight committee's primary set of duties which would involve evaluation of the risk framework and the methodology used for identifying and managing risk. Meanwhile, the duties of the specific committee members were indicated as general statements in the Charter. This includes attending meetings and general requirements regarding integrity.

He then sought the approval of the Committee for the Charter so that it may be adopted and made part of the Risk Oversight Committee's documentation.

Mr. Martin had a few comments on the Charter. In section four, the second sentence says that "*the Committee shall ensure that it maintains appropriate records*." He opined that this should be the responsibility of the corporate secretary rather than the Committee itself. Mr. Martin recommended to make this amendment to section four. Finally, He pointed to section seven, number one, on the duties and responsibilities of the members of the Committee, number one says "*accept the responsibility for creating and enhancing shareholder value and ensuring the long-term success and viability of Maxicare*". He suggested to revise and qualify this sentence by adding

"*...through the effective management of risk.*" This is to clarify that the role of the Committee is on enterprise risk management ("**ERM**") rather than any profit-generating effort. He had no further comments on the charter.

Mr. Panganiban moved for the approval of the Charter, subject to the amendments recommended by Mr. Martin. Upon motion made and duly seconded, the Charter was approved subject to the approval of the Board[3].

IV. DATA BREACH RISK ANALYSIS AND RECOMMENDATIONS FOR RISK ASSESSMENT

Lab@Home Breach

Atty. Fornier had an academic discussion on the data breach risk analysis regarding the Lab@Home data breach and notification. Upon review of the incident, SMT identified three (3) major risks: data security risk, regulatory compliance risk, and reputational risk.

Regarding the data security risk, Atty. Fornier noted that the compromised systems were not of Maxicare's, but of a third-party provider, Lab@Home. Thus, in so far as the system integrity of Maxicare's primary network was concerned, as well as cybersecurity measures, Maxicare systems remained uncompromised for the duration of the breach and to date.

This was marked green in the presentation indicating it was adequate or satisfactory in terms of MHC's approach. Meanwhile, the vigilance and competence of the management and staff was marked yellow because of

[3] It is noted that the BROC Charter, as amended was presented to the Board at its regular meeting held last 25 October 2024.

some challenges and delays in the handling of the data security of the investigation, and not because of competence, but probably lack of manpower. However, the third-party data protection regimes were an area that was evaluated to be an item that needed most improvement.

During the vetting of the third-party partners, security concerns were identified regarding their data storage practices and the competence of personnel handling sensitive information. Regarding regulatory compliance, most concerns were addressed satisfactorily.

Maxicare proactively assumed primary responsibility for data privacy liability and breach notification. On the other hand, data subject notification presented challenges. Despite efforts to reach all individuals, some were not notified timely. This was primarily due to inconsistencies in the contact information provided by the data subjects, rather than any lack of diligence on the part of Maxicare. Maxicare fully cooperated with the National Privacy Commission ("**NPC**") throughout their investigation. (Note: the NPC investigation was then currently under review). Maxicare would promptly inform all relevant parties of the NPC's final findings

Mr. Panganiban clarified whether the data breach was a phishing incident with Maxicare's third-party provider.

Atty. Fornier explained that the data breach was initially suspected to be a phishing attempt because the compromised access point was an email and password combination that belonged to a Maxicare employee. However, upon further review, it was characterized more as a "zero-day attack". He said that the IT experts described it as an "independent brute force compromise" of the portal from which they were able to obtain the access data. Atty. Fornier relayed that the employee involved in the data breach whose email and password access were compromised was investigated. After the employee was interviewed, the investigation committee was satisfied that it was not negligence on her part as she neither shared her email access nor clicked any unauthorized links. Therefore, the breach did not originate from her acts at any point. Rather, it was a "brute force attack" on Lab@Home's end and independent from Maxicare's server.

Mr. Panganiban asked how Maxicare's employees' email and password combinations were stored. Mr. Christian S. Argos ("**Mr. Argos**") responded that those data were encrypted. He narrated that upon forensic examination of the subject employee's phone and laptop, nothing in her email inbox was consistent with a phishing attempt and there was no link for her to click. There was no email or message on her phone, thus, no phishing attack was

detected. She also never logged into Lab@Home's system at any point and she did not even change her default password. Therefore, the theory was the breach was through a brute force attack on the default password because Maxicare employee's email addresses are very plain.

Mr. Argos also added to the discussion on the third-party data protection regimes (which were marked as red). He explained that Maxicare had safeguards in place and as an example, he explained that in order to access Maxicare's PayorLink, a VPN is needed on top of a multi-factor authentication, unlike Lab@Home. Mr. Argos pointed out that Lab@Home was not alone with its less stringent data protection protocols. He said that looking at the other thousands of Maxicare partner-hospitals and partner-clinics, Lab@Home's data protection was actually better with its VAPT assessment on their scheduling portal. Lab@Home even provided evidence and certificates that it went through an assessment and audit. On the other hand, most of the other partner hospitals and clinics of Maxicare do not have those.

Mr. Argos directed the discussion to the second major risk, Regulatory Compliance Risk, as follows:

He discussed the issue on the assumption of data privacy liability. He explained that it was still a question whether Maxicare was the actual personal information controller ("**PIC**") in this Lab@Home data breach incident. This was because the personal information was given by the Maxicare member directly to Lab@Home and Maxicare was merely the payor. Since it was a Maxicare member, Maxicare issued the letter of authority for its Lab@Home transaction. Therefore, he explained that there was a reasonable basis to state that Lab@Home was the actual PIC in this scenario. He also said that unpacking this would be more complex. This was why the third-party risk was highlighted in red.

Mr. Panganiban pointed out that since the risk lies with the third-party partners of Maxicare, he suggested to contractually regulate them. He explained that the contracts should remove Maxicare's accountability for breaches that involve Maxicare in the provider's respective data storage. He recommended that Maxicare should amend its contracts with these hospitals and clinics as soon as possible. Mr. Argos noted Mr. Panganiban's suggestions. He then explained that Maxicare had data-sharing agreements in place with several hospitals. However, these agreements primarily address data sharing originating from Maxicare.

Mr. Argos discussed that in order to enhance these agreements, a specific provision should be included outlining contractual remedies in the event of a data breach originating from the hospitals, particularly when company members or the company itself are impacted or if the hospital is the PIC.

It is crucial to acknowledge that even with contractual protections in place, Maxicare's reputation can still be significantly impacted by a data breach originating from a partner hospital. This reputational risk was evident in recent events, where the Maxicare was given media attention surrounding the data breach, despite not being the PIC.

To mitigate such risks effectively, it was recommended that Maxicare create a dedicated crisis management team, similar to the approach adopted by Cebu Pacific. This team would be responsible for swiftly responding to data breach incidents, actively engaging with the media, and proactively shaping the public narrative to minimize reputational damage. While minimizing legal risk is essential, proactive crisis management and reputational protection must be prioritized in future data sharing agreements.

Mr. Brian Go ("**Mr. Go**") shared his insights from the JG Summit side. He said that with the JG Summit's affiliates, JG Summit also encountered some similar issues. The stance JG Summit had agreed on was that the risk or the expectation of threat actors taking advantage of large organizations would always be there and it's not going to go away. He said that the companies should accept that breach would happen and the focus should be on the how the company would respond to it.

Mr. Martin asked a question whether Maxicare has the ability to influence or mandate minimum IT security standards for the third parties. Atty. Fornier affirmed that contractually, Maxicare can enforce such and this was actually something that Maxicare's clients tend to enforce against Maxicare. Before obtaining Maxicare as an HMO services supplier, the potential clients

typically mandate that Maxicare should have certain controls in place. Mr. Martin reiterated that MHC should explore on how to do the same.

Atty. Fornier then discussed the Reputational risks, viz:

Atty. Fornier discussed the mitigation remedies and disruption to member experience. He explained that the main item that could have caused harm was the disclosure of membership information. Therefore, the immediate action was to cancel the membership numbers of the affected subjects and then eventually reissue new membership cards, either electronically or physically, to the affected members. Unfortunately, there was an issue with that process and Maxicare was still verifying if this was done for all data subjects. In the meantime, Maxicare had been receiving complaints from certain members who were affected and who were still waiting for their new membership cards as they were unable to access their benefits. Atty. Fornier then pointed out that this was a reputational and service issue.

In response to Mr. Martin's question, Atty. Fornier confirmed that there were 17,120 Maxicare members who were affected by the data breach.

Aftermath Alignment

Atty. Fornier discussed the findings, assessment and understanding of what actually transpired, the first critical finding was that Lab@Home was the proper party to notify the NPC and undertake breach protocols. Firstly, Lab@Home was the collector of the data, even though the collection was under Maxicare's direction, because these are Maxicare members. There was no actual data transfer between Maxicare and Lab@Home. Therefore, Lab@Home was the one collecting the information. And thus, also, its systems were the ones that were compromised, so the Maxicare system and network were not touched during the attack.

He explained that the data subjects, while being members of Maxicare, were also concurrently Lab@Home's clients. Initially, Lab@Home was supposed to undertake a separate data breach notification, but after Maxicare was exposed with the responsibility for the breach, Lab@Home decided not to proceed and up to the date of this Committee meeting Lab@Home has not undergone any separate breach notification.

The assumption of the PIC role by Maxicare was possibly a necessary step for the mitigation of reputational risk because the Corporation was named and was the party that was threatened with the release of the information, even though the information was actually extracted from a separate party. Nonetheless, even though Maxicare took steps to assume responsibility and accountability, Maxicare's reputation may have been imperiled due to the disruption caused by remedial measures for the affected members. There were also certain delays in responsiveness to client member queries. This was because of the volume of clients across the 17,000 affected members who had expressed their concerns regarding the integrity of their data, even though, again, the data compromise was quite isolated and on the third-party server's end. Atty. Fornier explained that the members' concerns were reasonable considering the circumstances. Some of the worries of the clients were their credit card information and supposed accountability for possible credit card fraud.

Risk Management Strategy

Atty. Fornier then proceeded to discuss the risk management strategy of Maxicare moving forward. First, was to strengthen and reinforce third-party data security assessments to make them responsible for a minimum standard, two party authentication, data security, cybersecurity, protocols, encryption, and the like. In the contracts, Maxicare would likely add the requirement that all third parties, when they are clearly identified as the PIC, shall undertake the necessary legal steps to notify in accordance with the Data Privacy Act and the regulations of the NPC and failure to do so would result to penalty and a ground for contract termination. He said that it would be good to add teeth moving forward to future contracts with the third parties to ensure that once they are made PICs, they will take the responsibility and step in should there be a data breach.

The next strategy presented was the training and testing of system and staff and adequate staffing in the data privacy office and information security ("**InfoSec**"). Atty. Fornier said that Maxicare currently has no InfoSec office and there was only one person in the data privacy office of Maxicare. Thus, he recommended that given the importance of data security and protection,

it would be good to build the team into one that can more capably handle volume concerns, especially one such as this.

Mr. Cruz asked whether Maxicare had reviewed all the existing contracts with the third parties and whether the discussed safeguards can be added now or there was a need to wait for the renewal. Atty. Fornier responded that generally, contractual parties were reluctant to assume unilateral commitments unless they directly benefit from them. Consequently, this regime was likely to be perceived as burdensome by partners, and its implementation may not be feasible until contract renewal. Therefore, it was crucial to maintain vigilance and thoroughly review and overhaul each agreement during the renewal process to ensure the inclusion of necessary safeguards.

Mr. Argos provided his inputs to the discussion. He said that Maxicare recently renegotiated a vast majority of its contracts from the perspective of putting in additional protection for claims and cost and that was very contentious. He said that they have been working on it for over a year, to the point where this had delayed the execution of some contracts and led to suspensions and disaffiliations because of these contentious items. According to Mr. Argos, this was going to be a risk management exercise in its true form and focus on the major providers that handle most of the volume of Maxicare members, but then, whether big or small, a breach is a breach. He opined that even the smaller clinics have equal levels of risk if their data is breached and compromised as far as the impact on Maxicare is concerned. Based on the foregoing, he concluded that there was no definite answer yet, but Maxicare would go with the same route as what was done last year focusing on POS (point-of-service). He also pointed out that some of the third parties have no data security measures in place.

Mr. Cruz commented that at least it's best to know what the risks were than not knowing. This could be factored in when looking at other providers moving forward.

Mr. Martin suggested that Maxicare could have a set of acceptable minimum standards, against which can be used to cross-reference all Maxicare's counterparties and vendors in terms of cybersecurity and IT security. This could be used to gauge and measure who among Maxicare's counterparties were up to the standard and who was falling below that particular standard. Atty. Fornier acknowledged this suggestion.

Mr. Panganiban raised the concern of criminal liability regarding the data breach and Data Privacy Act violations. He suggested that should these

counterparties disagree with the contractual arrangements regarding the cybersecurity and data protection protocols, Maxicare should point out the criminal liability attached then they would be compelled to follow the law. Mr. Martin agreed with Mr. Panganiban and added that Maxicare should also point out to counterparties that lack of protection in their own systems would be gross negligence on their end.

Lastly, the final strategy Atty. Fornier presented was the development of breach assessment policy. He said that it would be beneficial to develop a consistent breach assessment policy. This policy would enable a systematic evaluation of any similar event, determining whether it constitutes an actual breach as defined by the NPC and assessing Maxicare's responsibility. A crucial distinction exists between transferring data from Maxicare's systems to third-party systems, establishing the organization as the PIC, and instances where third parties independently obtain information, even if under Maxicare's guidance or due to Maxicare's service to its members. In such cases, careful evaluation is necessary before initiating breach response procedures. Subsequently, a standardized procedure should be established for handling future data breach situations.

Ms. Rizalina Mantaring ("**Ms. Mantaring**") asked who was on the crisis management team of Maxicare. Mr. Argos said that there was an ad hoc committee and it was the entire executive leadership team ("**ELT**"). The team was spearheaded by two personnel, one from the operations side, which includes the ICT, and one from the external side. In the ICT, it was Allen Tatco and Ned Cayetano, when he was still the Chief Technology Officer. They were handling that track and engaging Lab@Home. For the external communications, it was Mr. Archie Rillo who coordinated with Atty. Renato Salud of JG Summit's government and public relations office.

Ms. Mantaring suggested to constitute a formal crisis management team. She added that the crisis management team usually does not have the executive team in it, except probably the team leader. This would make the executive team free to make decisions whenever a crisis happens. She also suggested that there should also be a spokesperson formally appointed for similar situations.

Mr. Martin requested for Mr. Argos to look into Ms. Mantaring's recommendation and come up with a proposal addressing those discussed. Mr. Argos agreed and he explained that this was in line with the SMT's focus. He also recounted their visit at Cebu Pacific's office where there was a crisis management room. In the room were all the manuals and procedures in case of a crisis, and the members of the crisis team were already set. In case of a

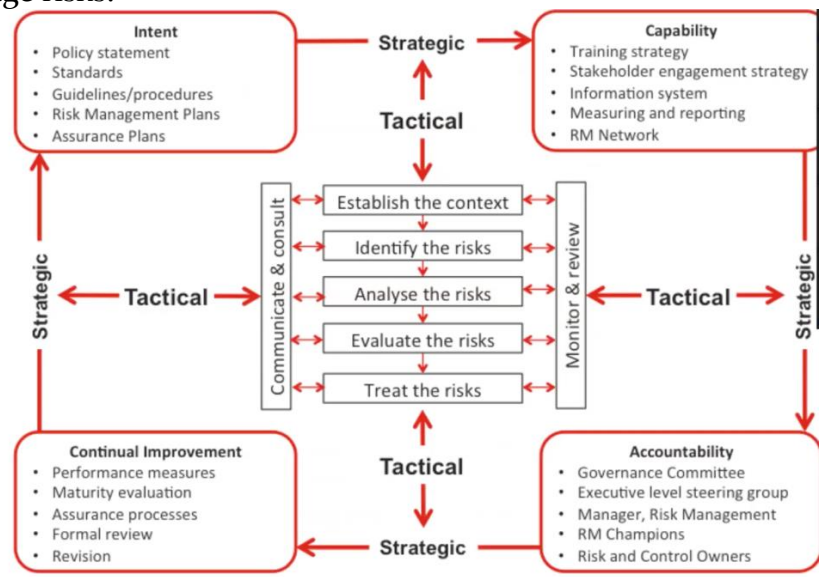
crisis, the crisis team would go into the room and go through the playbooks. Ms. Mantaring commented that despite having playbooks it is impossible to anticipate all possible crises, thus, the crisis management team should nonetheless be able to think on their feet and make quick decisions.

Mr. Cruz added that it is anticipated that potential gaps in business continuity and crisis management will be identified as the organization embarks on its enterprise risk management ("**ERM**") framework. These areas should be integral components of the comprehensive ERM framework, guiding the development of contingency plans and crisis management strategies. Furthermore, Maxicare should prioritize training its leaders in crisis management and business continuity principles. A potential approach to enhance efficiency and ensure consistency across the Maxicare Group of Companies is to implement these training initiatives as a group initiative, leveraging economies of scale. Mr. Argos noted this and he suggested borrowing and leveraging capability from the JG Summit side. Mr. Cruz furthered that there are parties that engage in this training, and it is a continuing training program.

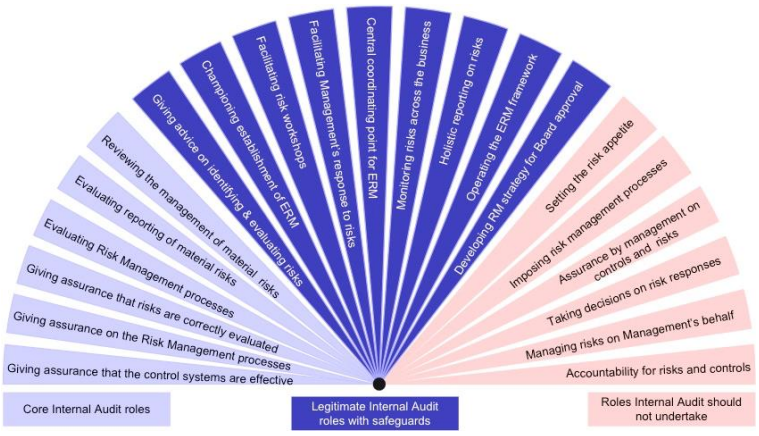
V. INITIATORY ACTIONS FOR ERM FRAMEWORK

Atty. Fornier discussed some rudimentary aspects of ERM. He also discussed the distinction between audit and risk because according to him, often the concepts tend to overlap.

He presented the framework from the ISO 31000 guidelines on how to manage risks:



Atty. Fornier presented the diagram below to show the functions of audit.



The diagram showed the roles of internal audit and those which the internal audit should not take as these were usually within the province of risk. The middle area reflected the areas where audit and risk functions overlap. However, according to Atty. Fornier, the recommendation of current related literature was for the middle area of the diagram to be assumed likewise by risk.

Mr. Martin commented that it was good to distinguish risk and audit because risk should be the second level of defense and audit was the third line of defense. He added that audit should be revisiting or reviewing risk as well.

Atty. Fornier then presented the distinct roles of risk and audit:

The distinct roles of Risk and Audit

RISK

- Develop and implement the Risk Management Framework (RMF)
- Advise on RMF roles, controls, tasks and accountability
- Advise on interpretation of risk management information
- Provide appropriate risk management status and performance information
- Acts as advisor and mentor for risk management matters

AUDIT

- Audit the adequacy and effectiveness of the RMF
- Audit commitment and capability of accountable officers to RMF roles
- Provide independent assurance of risk management information
- Assess credibility and reliability of risk management information
- Independent reviewer of management's capability and performance in risk management

He discussed that the risk management function will be responsible for developing and implementing the ERM framework, including defining roles, establishing controls, and executing risk management tasks. They will interpret information, provide status updates, and act as advisors to business units.

Meanwhile, the audit function will independently assess the effectiveness of the risk management function, evaluate risk assessments, and assess the performance of risk owners. By clearly defining these roles, the organization will ensure improved risk management effectiveness, enhanced risk awareness, and increased confidence in the accuracy of risk information. This framework will provide a strong foundation for a robust and effective risk management culture.

Atty. Fornier then discussed the framework building process. This will commence with initial steps such as process identification and would involve conducting interviews, performing walkthroughs, and potentially organizing workshops with key internal stakeholders. End-to-end process mapping across divisions will be undertaken to identify points of exposure and assess the effectiveness of existing internal controls in mitigating these vulnerabilities. This analysis will ultimately contribute to the development of the risk register.

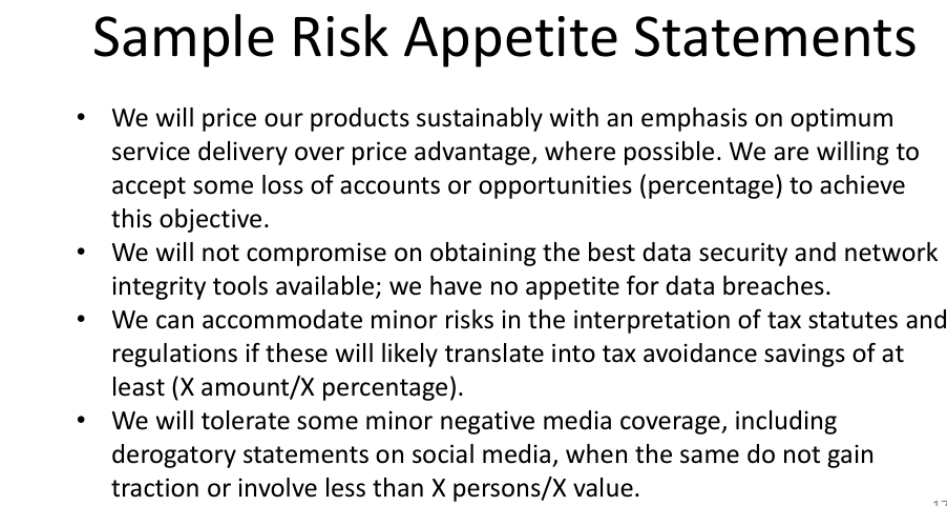
Atty. Fornier presented the risk register, which will primarily focus on high-impact (red) and medium-impact (orange) risks. Residual risks, those with low probability or minor business impact, will be considered, but may not require the same level of immediate attention.

Probability			Business impact				
			Extreme	Major	Moderate	Minor	Insignificant
			Complete operational failure, "bet the farm" impact, unsurvivable	Severe loss of operational capability, highly damaging and extremely costly but survivable	Substantial operational impact, very costly	Noticeable but limited operational impact, some costs	Minimal if any operational impact, negligible costs
			100%	80%	62%	25%	1%
(Almost) certain	We are *bound* to experience further incidents of this nature - in fact they are probably occuring right now!	100%	100%	80%	62%	25%	1%
Probable	We are likely to experience incidents of this nature before long	80%	80%	64%	50%	20%	1%
Possible	It is distinctly possible that we will experience incidents of this nature	62%	62%	50%	38%	16%	1%
Unlikely	Incidents of this nature are uncommon but there is a genuine chance that we may experience them at some future point	25%	25%	20%	16%	6%	0%
Rare	Although they are conceivable, we will probably never experience incidents of this nature	1%	1%	1%	1%	0%	0%

Ms. Mantaring commented on the roles of risk and audit. She emphasized that there should be coordination between the two on what should be audited because audit should be risk-based. She added that the frequency of audit should also be based on the level of risk. Regarding the risk register, she made a minor comment that usually with other organizations, it was green on the bottom left and the red on the upper right.

Mr. Cruz added to Ms. Mantaring's comment on having a risk criteria. He said that there is no risk-free environment, hence, corporations should have proper risk identification, risk assessment, and a risk acceptance criteria.

Atty. Fornier then proceeded to discuss the Corporation's risk appetite. Atty. Fornier sought guidance from the Committee on the risk appetite or tolerance of Maxicare. He presented some sample risk appetite statements for consideration and refinement.



These statements will serve as a foundational guide for the development of the risk management framework, providing clear parameters for acceptable risk levels across different risk categories. Some risk categories may have zero tolerance, while others may allow for low to moderate levels of risk. Risks deemed less critical may be managed on an ongoing basis as they arise.

Atty. Fornier said that he intends to present a risk sliding scale in the next Committee meeting.

In future meetings, Mr. Panganiban suggested that Atty. Fornier present a detailed plan for formalizing the ERM system across the organization. He understands that the presentation was an initial step that outlined the implementation roadmap, starting with the development and

implementation of the ERM framework. He furthered that the plan for the ERM system should address organizational structure and roles, including the identification and appointment of risk champions and their respective areas of responsibility. The plan for the ERM system should also detail the training and development program, outlining the approach (e.g., top-down, bottom-up, or a combination) and the training schedule for leaders and team members. The plan should also include a methodology for identifying and prioritizing top risks, likely involving a combination of top-down and bottom-up approaches to gather comprehensive risk information. Finally, he suggested that Atty. Fornier should include a timeline and key milestones to track progress toward the successful implementation of the ERM system.

Atty. Fornier noted Mr. Panganiban's suggestions and affirmed that these matters were being considered. He discussed that a critical step in developing an effective ERM system is to gain a thorough understanding of the organization's processes by engaging with internal stakeholders. Direct interaction with employees will provide valuable insights into the risks they encounter on a daily basis, their risk management practices, and their anticipated challenges. This firsthand knowledge will be crucial in identifying and prioritizing key risks across the organization. Based on this initial risk assessment, the organization will determine the most appropriate implementation approach for the ERM system.

Since the discussion was risk in general terms, Mr. Martin suggested that in the subsequent meeting for Atty. Fornier to identify specifically the types of risks that are intended to be covered (i.e. credit, liquidity, interest rate, reputational, information security, and operations). This was duly noted by Atty. Fornier.

VI. 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