BPI/MS
A-3 Enterprise Risk Management

Version 4.0

(Ref: MSIG Asia A-3 V9)
Board informed

Table of Contents

Chapter 1: The Policy

Version 3.0

1. Purpose

1.1. This document is the primary policy document outlining BPI/MS' Enterprise Risk Management ("ERM") objectives and its underlying requirements.

2. Applicability

2.1. In case of a conflict between this document and any applicable local regulations, local requirements take precedence.

3. Effective Date

3.1. This document is effective from September 17, 2020.

4. Documents Superseded

4.1. This policy document supersedes the following guidelines and policy documents for BPI/MS:

- *G-RMD-008 ERM Basic Rules*
- *G-RMD-004 BPI/MS Risk Management Policy*
- *BPI/MS Strategic Risk Management Framework*

5. Objectives of Risk Management

5.1. The key objectives of ERM in BPI/MS are as below:

- Develop and maintain an ERM process as an integral part of the insurance operation to support sustainable business growth
- Provide transparency in risk assessment to relevant stakeholders
- Protect local solvency and maintain financial sustainability
- Provide the platform required to develop a sustainable risk management framework
- Clearly define ownership and responsibilities for identifying, assessing, managing risks
- Create an effective risk management culture in BPI/MS

6. BPI/MS ERM Framework

6.1. BPI/MS' ERM framework exists to provide the infrastructure within which risk governance and accountability reside and also sets out the processes required to sustain risk management within BPI/MS and deliver the overall objectives of BPI/MS' risk management as outlined above.

6.2. BPI/MS is required to develop and maintain the following ERM components under the MSIG Asia ERM framework:

- Risk appetite framework
- Capital management plan
- Solvency assessment
- Stress testing
- Comprehensive risk assessment
- Risk monitoring and reporting

6.3. Any material changes to the ERM framework require prior consultations with MSIHO and approval of Risk Management Committee ("RMC") and Board of Directors ("BOD").

7. Roles and Responsibilities

7.1. The BOD is ultimately responsible for ensuring that BPI/MS maintain an appropriate level of capital for their risk profile and business plan.

7.2. RMC, supported by Risk Management Working Committee ("RMWC") and risk management function, is responsible for the development and effective implementation of the risk management framework.

8. Non-compliance

8.1. In case of non-compliance with the requirements set out in this policy document, the BPI/MS' policy owner is required to request for a dispensation from the MSIHO policy owner in writing.

8.2. Approved dispensations are required to be reported to the relevant risk committees of BPI/MS and MSIHO.

9. Policy Management

Policy owner

Policy owner in BPI/MS is responsible for issuing and maintaining this policy.

Merlina P. Mendoza
Director, Finance and Risk Management Department
BPI/MS Insurance Corporation
mpmendoza@bpims.com
+63 (2) 840-59701

Policy manager

Policy manager in BPI/MS is responsible for assisting the policy owner in discharging responsibilities under this PRGs.

John Victor Q. Buena
Risk Management Support Officer
BPI/MS Insurance Corporation
jvqbuena@bpims.com
+63 (2) 884-09779

Policy advisor

Policy advisor is appointed by MSIHO to support MSIHO and BUs in the management and execution of this PRG.

Policy advisor, with the related knowledge, expertise and experience, shall provide counsel, recommendations and advice to MSIHO on matters related to the management and execution of the respective PRG and facilitate communications between MSIHO and BUs

William Song

Chief Risk Officer

MSIG Holdings (Asia) Pte Ltd

William_song@msig-asia.com

DID +65 6827 7855

Chapter 2: The Regulation

Version 3.0

1. Basis

1.1. This section outlines the specifications of the BPI/MS ERM Framework.

1.2. The requirements in this section are mandatory unless a dispensation is granted by the Regional Policy Owner in MSIHO.

2. Committee

2.1. BPI/MS is required to set up and maintain a dedicated risk management committee at the board and management level ("the Committees").

2.2. The main responsibilities of the committees are as below:

2.2.1. Risk Management Committee ("RMC") – Board level committee

- Develop, implement, and oversee the Risk Management program of BPI/MS Insurance Corporation.
- Identify, assess and manage risk exposures.
- Monitor and oversee the Capital Management program.

The committee must at least include the following members:

- At least four (4) members of the BOD, two (2) of whom shall be independent directors
- The Committee Chairman must always be an independent director

2.2.2. Risk Management Working Committee ("RMWC") – Management level committee

- Promote, develop, and maintain a best practice of ERM framework
- Identify, assess, and manage relevant and material risks in the company and region to ensure alignment with the regional strategy
- Assess capital adequacy to meet statutory and capital requirements of BPI/MS

- Report key risk assessments to appropriate stakeholders, as necessary
- To ensure compliance with relevant risk management regulatory requirements as mandated by Bank of the Philippine Islands (BPI) and MSIHO
- Support the RMC

The committee must at least include the following members:

- Chief Executive Officer or equivalent
- Chief Financial Officer or equivalent
- Head of Risk Management or equivalent
- Other functional leaders from the operation as necessary

2.3. The committees are required to meet up at least on a quarterly basis to review the following key issues:

- Business risk profile
- Solvency assessment
- Other ERM activities, including regulatory requirements

2.4. The committees are responsible for the review of various Risk Management policies, including but not limited to, Capital Management Plan, Risk Appetite Framework, and Related Party Transaction Policy.

2.5. The RMC is required to update the board of directors on the key issues and summary of the risk management committee meeting at least on a half yearly basis.

3. Risk Appetite Framework

3.1. Risk appetite is amount of risk an organization is willing to accept in pursuit of its corporate objectives and the risk appetite statement of articulates the risk and reward trade-off behaviour of the organisation.

3.2. The board of directors are ultimately responsible for setting the risk appetite and to ensure its alignment with the corporate strategy and mid-term business plan.

3.3. BPI/MS ERM function is required to set up and maintain a document articulating the risk appetite framework and the statements.

3.4. Risk appetite statements must factor in the following key risk categories:

- Underwriting risk
- Reserving risk
- Market risk
- Credit risk
- Liquidity risk
- Operational/Other risk

3.5. The RMC is required to assess the general consistency of risk appetite statements with the latest business plan and practice on an annual basis.

3.6. The RMC is required to review the risk appetite framework and the statements on an annual basis.

3.7. The status of the review, including any material changes, is required to be reported to the board of directors on an annual basis.

3.8. Any changes to the company level risk appetite framework and the statements, i.e. Risk Capacity and Risk Appetite (exclusive of Risk Tolerance), require consultation with MSIHO and Policy Advisor prior to the approval by the board of directors.

4. Capital Management Plan

4.1. Capital management plan ("CMP") is a process of setting and managing the insurer's financial resources and strength. This includes taking into consideration the entity's business and risk profile, with an objective of ensuring sustainable financial soundness and robustness.

4.2. The board of directors are ultimately responsible for determining the target operating range of the capital, which may vary depending on the level of risk faced by the insurer.

4.3. BPI/MS ERM function is required to set up and maintain a document articulating the capital management plan.

4.4. The capital management plan must be set based on the local solvency framework.

4.5. The capital management plan must include the following solvency trigger points:

- Minimum statutory solvency requirement
- Any solvency notification levels as required by the local regulator, if applicable
- Internal solvency trigger point above the notification level
- Target operating range of capital

4.6. For each of the solvency trigger points, RMC is required to agree and document appropriate management actions to restore and maintain sufficient solvency in case of a breach.

4.7. RMC is required to review the capital management plan:

- on an annual basis; or
- if there are changes to local solvency requirement; or
- if there is significant change to the risk profile.

4.8. The status of the review, including any material changes, is required to be reported to the board of directors on an annual basis.

4.9. Any changes to the capital management plan require consultation with MSIHO and Policy Advisor prior to the approval by the board of directors.

5. Solvency Assessment

5.1. Solvency assessment is a process to review the adequacy of current and future capital requirement of an insurance entity.

5.2. The board of directors are ultimately responsible to ensure the capital adequacy on an ongoing basis.

5.3. The capital adequacy is required to be assessed with respect to the local solvency requirement.

5.4. RMC is required to conduct a review of solvency assessment, reflecting the following components:

- Past solvency trend
- Current solvency position
- Projected solvency requirement based on the latest business plan and any relevant latest available information
- Anticipated seasonality in solvency position during the year
- Expected dividend payment
- Any expected changes in the solvency regulation

5.5. RMC is required to monitor the solvency position on a quarterly basis.

5.6. The projection horizon is required to be at least 12 months.

5.7. Best estimate projected solvency position over the projection horizon should not result in breaching the local solvency requirement or the regulatory notification level.

5.8. RMC is required to conduct solvency sensitivity analyses on an annual basis in order to identify the key parameters that may have material impact on the overall solvency position, both current and future, of the entity.

5.9. RMC is required to report the key findings from the solvency assessment to the board of directors at least on an annual basis.

5.10. The Policy Advisor is required to review the reports and provide the necessary assessment.

6. Stress Testing

6.1. Stress testing is a risk management process to assess the financial robustness of an insurance company against extreme but plausible events.

6.2. The board of directors or equivalent are ultimately responsible to assess the reasonableness of stress scenarios and the estimated impacts.

6.3. RMC is required to conduct stress tests considering at least the following scenarios:

- Macroeconomic shock
- Large insurance loss
- Reinsurance default of a major reinsurance counterparty following a large loss or a natural catastrophe event
- Natural catastrophe event with a return period of 1-in-200 years

6.4. Stress tests are required to be conducted on local solvency requirement.

6.5. RMC is required to conduct stress tests on an annual basis.

6.6. The key findings from stress tests are required to be reviewed by the RMC.

6.7. The results, including necessary mitigating actions, are required to be reported to the board of directors on an annual basis.

6.8. RMC is required to develop necessary corrective actions against identified events, if the stress scenarios are deemed to be unacceptable.

7. Comprehensive Risk Assessment

7.1. Risk assessment is a risk management process to identify, assess and manage risks that are relevant to the organisation.

7.2. BPI/MS ERM function is required to set up and maintain the following documents with the necessary consultation from MSIHO and Policy Advisor:

- Risk register; and
- Business risk profile.

7.3. Risk register is the list of risks that are relevant to the organisation but may not necessarily be material.

7.4. BPI/MS is required to review and update the risk register every six months.

7.5. Business risk profile is the summary of relevant and material risks from an organisation's perspective.

7.6. All risks identified in the business risk profile are required to have the following components:

- Risk description
- Risk owner
- Estimated impact category
- Estimated likelihood category
- Key risk indicator
- Risk controls
- Key control indicator
- Control effectiveness indicator
- Future mitigating action with estimated impact and likelihood, if necessary

7.7. A template of the risk profile summary is provided in Appendix E.

7.8. Assessment of the following components should be in line with the definitions provided in Appendix F:

- Estimated impact category
- Estimated likelihood category
- Control effectiveness indicator

7.9. Risk owners are required to review and update the risks included in the business risk profile on a quarterly basis.

7.10. RMC is required to review the business risk profile, including relative positions of each risk, on a quarterly basis.

7.11. The key summary of the business risk profile is required to be reported to the board of directors on a quarterly basis.

7.12. BPI/MS ERM function is required to submit business risk profile reports to MSIHO on a quarterly basis.

7.13. BPI/MS has a Strategic Risk Management framework which shows the integration of risk management into the strategic planning process.

7.14. The BPI/MS Strategic Risk Management framework is provided in the Appendix C.

7.15. BPI/MS is using a risk management tool called Risk Assessment for Business Activities (RABAct) which shall be conducted to provide information on the potential or anticipated risks prior to the implementation of:

a. New or changes to existing business activities (e.g. markets, product, business process/sytem)
b. Exception handling /deviations from existing policy, standards or guidelines.

7.16. The RABAct guideline is provided in the Appendix D.

7.17. The Policy Advisor is required to review the reports and provide necessary assessment.

8. Risk Monitoring and Reporting

8.1. The following items are required to be reported and discussed by the RMC and the board of directors on a quarterly basis:

- Material risk profile
- Solvency assessment
- Any other key matters related to ERM

8.2. BPI/MS ERM function is required to submit the Risk Monitoring Report to MSIHO on a quarterly basis.

8.3. The Policy advisor is required to review the reports and provide necessary assessment.

Chapter 3: The Guideline

Version 3.0

1. Basis

1.1. This section provides guidance which may consist of information intended to promote best practice ERM.

1.2. This section is not mandatory; however, BPI/MS is encouraged to adopt relevant sections as deemed appropriate.

2. Emerging Risk Management

2.1. MSIG defines emerging risk as "*unregistered risks that are newly developing or changing which may not be fully understood and which may have a major impact on an organisation*".

2.2. Emerging risk management and reporting serves as an early-warning system and is characterised by a high degree of uncertainty.

2.3. BPI/MS and MSIHO are recommended to consider the following categories for their emerging risks:

- Nature of impact: social, technological, environmental, political, business, economical
- Time horizon: 0-3 years, 3-5 years, beyond 5 years
- Affected classes of business or function

2.4. BPI/MS and MSIHO may consider developing management actions to mitigate the identified emerging risks.

2.5. It is recommended that BPI/MS discuss any potential emerging risks at the quarterly risk committees.

3. Own Risk and Solvency Assessment

3.1. The Own Risk and Solvency Assessment ("ORSA") is a framework to summarise the process, outcomes and the capital position and the underlying risks of an insurance entity.

3.2. It sets out the overall solvency and capital needs for the reporting period as they pertain to its business strategies, and objectives, related inherent risk profile and risk bearing capital capacity and Board approved risk appetite

3.3. BPI/MS is recommended to prepare and review the ORSA report on an annual basis, covering the following key issues:

- Current risk assessment
- Solvency assessment
- Forward-looking assessment
- Areas of enhancement

3.4. A sample structure of the ORSA report is provided in the Appendix A.

4. Three Lines of Defence

4.1. Three lines of defence is a risk management concept to ensure effective independence and oversight through the operation of three separate layers of defence with clearly defined responsibilities.

4.2. The first layer of decision making associated managing risks rests with functions that manage or accept risk on behalf of the organisation.

4.3. These functions typically are:

- Underwriting and their management
- Claims
- Investments
- Finance
- IT & Operations

4.4. The second line of defence is based on advice, monitoring, and challenge of the risk decisions and actions of those in the first line.

4.5. This is typically done by the following functions:

- Compliance
- Legal
- Risk

4.6. The third line of defence is typically covered by the Internal Audit which independently reviews both the first and second line functional controls and reports directly to the audit committee.

4.7. BPI/MS is encouraged to clearly develop and identify the three lines of defence framework in consultation with MSIHO and Policy Advisor.

5. Communication

5.1 Communication such as inquiries, requests (including dispensation request), reports and supporting documentation related to the respective PRG between MSIHO and BUs shall be made through or copied to Policy Advisor.

Appendices

Appendix A: Sample ORSA Report Structure

Appendix B: Dispensation request template

APPLICATION FOR DISPENSATION FROM AN MSIG ASIA POLICY

MSIG Asia Policy Dispensation Requested For	
BU Requesting Dispensation	
BU Policy Coordinator	
BU Policy Owner	

Area(s) covered by Policy for which dispensation is requested	
Reason(s) why BU cannot comply with the MSIG Asia Policy	
State whether dispensation requested is permanent or transitional, with reasons. Where transitional dispensation is requested, give timetable for compliance.	
If permanent dispensation is requested, what alternative(s) could be adopted?	
Highlight any regulations that compliance with the MSIG Asia Policy could violate.	

Regional Policy Advisor	
Recommendation/Advice	

MSIHO Policy Owner	Yoshiaki Okajima, General Manager and Head of Asia Section, International Business Dept.
Dispensation granted?	YES / NO
Permanent or transitional?	PERMANENT / TRANSITIONAL
Additional comments or explanation by MSIHO	
Date this dispensation expires (if any)	

Notes for completion
Be as specific and detailed as possible in requesting dispensation: help the MSIHO PO understand why you cannot comply.
Where transitional dispensation is requested, give realistic timetables.
Where there are regulatory issues in complying, give potential penalties etc
If there is any additional information or supporting documentation that you can give this may be supplied under separate cover.

MSIG Holdings (Asia) Pte Ltd
Regional Holding Company

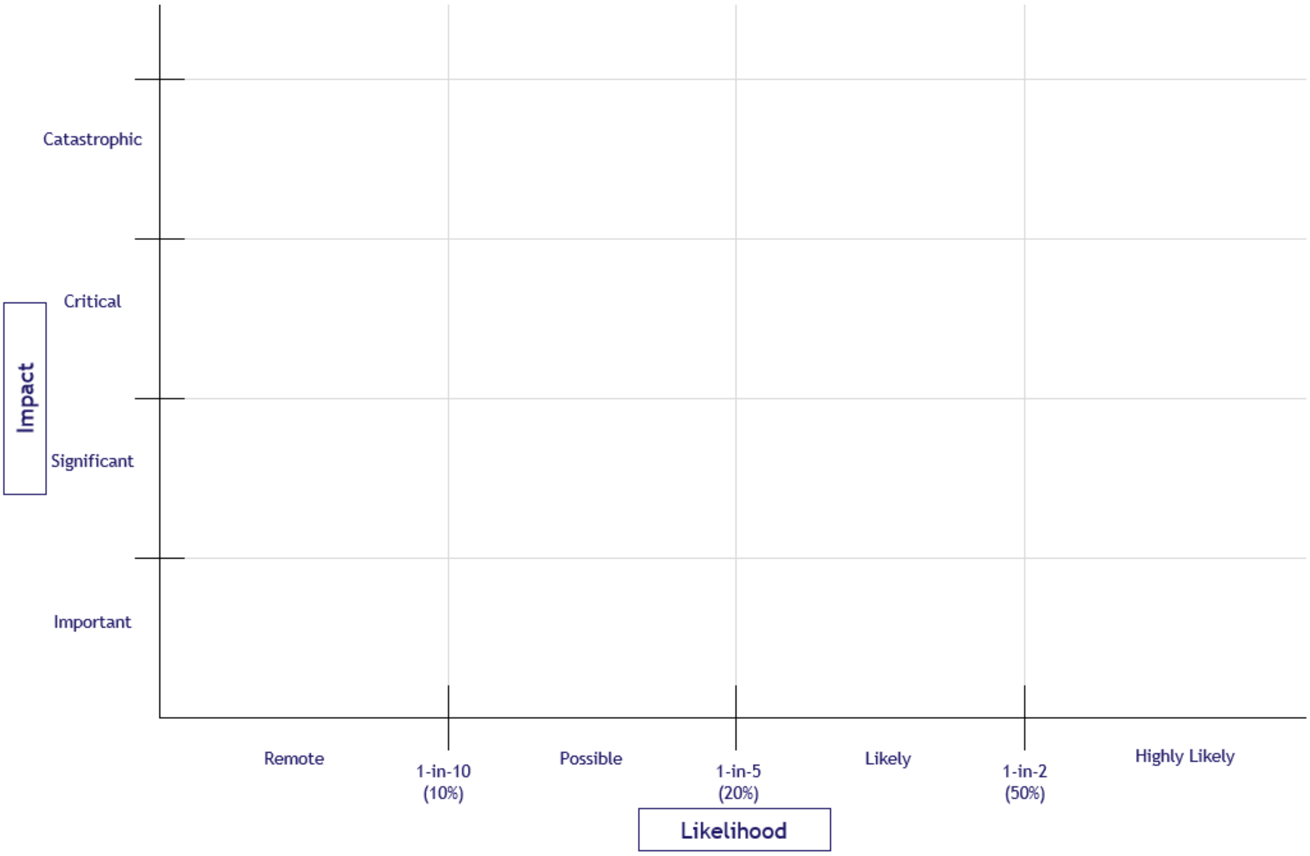
Appendix C: BPI/MS Strategic Risk Management Framework

Strategic Risk
Management Frame

Appendix D: Risk Assessment for Business Activities Guidelines

BPIMS Risk
Assessment for Busi

Appendix E: Risk Profile Summary Template



Appendix F: Risk Profile Definitions

1. Estimated impact categories

	Financial	Regulatory	Reputational	Operational
Catastrophic	Severe loss in capital, resulting in statutory insolvency and requiring an immediate capital injection; and/or Permanent loss in gross premium in excess of 50 per cent of the total portfolio	Regulatory sanctions resulting in a revocation of insurance license or a temporary cessation of new business	Immediate and permanent damages to the reputation and trust of MSIG involving the media, leading to a loss of confidence from customers, intermediaries, business partners and shareholders	Immediate and prolonged disruption on critical operations including but not limited to, underwriting, policy processing, claims management and finance
Critical	Material impact on the financial condition of the business unit; however unlikely to result in statutory insolvency; or Temporary insolvency without loss of capital; and/or Permanent loss in gross premium in excess of 20 per cent of the total portfolio	Regulatory sanctions resulting in a financial penalty in excess of 5 per cent of net asset	Negative impact to the reputation and trust of MSIG involving the media, leading to a loss of confidence from customers, intermediaries, business partners and/or shareholders; however recoverable at a considerable cost	Disruption on critical operations, including but not limited to, underwriting, policy processing, claims management and finance
Significant	Adverse impact on the financial performance of the business unit that will make it difficult to achieve the overall business plan	Regulatory sanctions resulting in financial penalties of less than 5 per cent of net asset	Negative impact to the reputation and trust of MSIG, including a viral effect on social media, leading to a loss of confidence from a segment of customers, intermediaries, business partners and/or shareholders; however recoverable with time and PR support	Immediate and prolonged disruption/impact on operations; however without impacting day-to-day business
Important	Adverse impact on the financial performance of the business unit; however recoverable and will not threaten the performance against the overall business plan	Regulatory sanctions not involving financial penalties	Negative impact to the reputation and trust of MSIG leading to a loss of confidence from customers, intermediaries, business partners and/or shareholders	Disruption/impact on operations; however without impacting day-to-day business

2. Estimated likelihood categories

Probability of occurrence in 12 months	Event Likelihood	
Remote	<10%	Lower than 1-in-10 years
Possible	Up to 20%	1-in-5 years
Likely	Up to 50%	1-in-2 years
Highly Likely	>50%	Higher than 1-in-2 years

3. Control effectiveness indicator

Control effectiveness indicator serves to represent the management's assessment of the control effectiveness.

Green: Fully effective controls

Management believes controls are effective and reliable. "Nothing more to be done except review and monitor the existing controls"

Yellow: Largely effective controls

Most controls are designed correctly, are in place and effective. Some more work to be done to improve effectiveness or management has some doubts about operational effectiveness and reliability. "Most things in place and working, but some more still to be done"

Orange: Partially effective controls

Some controls in place but are only partially effective with potentially material gaps. "About half way there"

Red: No or ineffective controls

No credible control or management has no confidence that any degree of control is being achieved due to poor control design or very limited operational effectiveness. "Just getting started"