BPI / MS Insurance Corporation

A joint venture of Bank of the Philippine Islands and Mitsui Sumitomo Insurance

# BPI/MS

# Risk Management Policy

Version 3.0
G-RMD-004
2017

# Revision History Summary

| Version | Effective date | Description of Change |
|---|---|---|
| 1.0 | March 6, 2010 | Initial Issue |
| 1.1 | September 1, 2012 | Change in Asset Management Risk Portion (BPI/MS Risk Management Policy)<br><br>- Annually, at the Board of Directors' fourth quarter meeting, AMTG shall present to the Board for its review the performance of the investment portfolio and the recommended strategies and outlook for the future. |
| 2.0 | December 4, 2014 | Adoption of MSI Risk Management Framework but will still observe and comply with requirements of the BPI Risk Management Office. |
| 3.0 | July 1, 2017 | Change in policy owner and manager<br>The use of term Compliance and Risk Management Working Committee was changed to Risk Management Working Committee<br>Change in document code from G-RMD-04 to G-RMD-004 |

ENDORSED BY:

| | | |
|---|---|---|
| MASAYUKI TAKHASHI | KOICHIRO KAWASAKI | MA. PERPETUA A. CUTIONGCO |
| YASUHIRO KANO | ANTHONY LOU M. BERNABE | NESTOR MAURICE JR. C. DANTES |
| ALBERTO C. SANTOS JR. | DANIELLE MARIA SALES-TORT | MERLINA P. MENDOZA |

# CONTENTS

# The Policy

## Version 3.0

MSIG Asia will have a robust and consistent set of procedures in place to ensure a strong risk management culture exists in all operations; and that all material risks are identified, evaluated and, where necessary, effectively mitigated. BUs (Business Units – under this Policy BPI/MS), will only accept risks where the reward is greater than the cost of carrying the risks, and will only accept those risks within the Groups risk appetite.

# 1. Objectives

1.1 MSIHO is responsible for setting and regularly reviewing the Groups risk appetite. This is communicated through the MSI Risk Management Policy and Guidelines for Overseas Operations, which sets the standards upon which this Policy is based, and is attached for further guidance. In the unlikely event that a situation is not covered by this Regional Risk Management Policy, BPI/MS should refer to the MSI Risk Management Policy and Guidelines for Overseas Operations.

1.2 BPI/MS Senior Management is responsible to their Board for risk management within their operating unit. Operational management must continually assess and manage risk as it affects the company, and escalate changes in the risk profile to their Board and RHC as necessary.

1.3 Reporting of risks and of changes in risk profiles along with actions to control those risks is a positive part of effective management. The Company believes in a culture of 'no surprises' and early notification of potential new risks or changes in risk profile is mandatory.

1.4 Risk should be managed and controlled effectively and appropriately rather than to attempt to eliminate it totally. This will enable a level of risk to be taken on that will optimize returns. Risk taking is fundamental to an insurance company but it must always be in a manner that will not jeopardize BPI/MS' solvency or reputation.

1.5 The above notwithstanding, BPI/MS will continue to observe and comply with the requirements of the BPI Risk Management Office (BPI RMO).

# 2. The Policy

## Principle 1 – Risk Defined

A Risk is defined as something that may prevent BPI/MS from sustainable achievement of its objectives, both in financial and non-financial terms, including the Group being prevented from fully exploiting opportunities.

## Principle 2 – Risks Covered by This Policy

This Policy covers risks arising from:

1. Internal sources that is internal control failures; and

2. External sources:

    2.1 Regulatory changes
    2.2 Government actions or changes of government
    2.3 Economic changes
    2.4 Competitors actions

## Principle 3 – Roles and Responsibilities of the BPI/MS Board and Management

The local Board will set the BPI/MS' level of risk appetite, and monitor Risk Reports from the BPI/MS Management Team.

The local Board is also responsible for Asset Liability Management (ALM) in order to achieve BPI/MS financial targets, given its risk appetite and other constraints.

## Principle 4 – Roles and Responsibilities of BPI/MS Senior Management

BPI/MS Senior Management is responsible for identifying, measuring, assessing, monitoring and reporting risks, and for putting in place effective mitigating controls where desirable. Risks across the entire business operations must be considered.

## Principle 5 – Formation of a Risk Management Committee

BPI/MS Senior Management is responsible for forming a Risk Management Committee to consider risk and to assist them in discharging their responsibilities under this Policy.

## Principle 6 –Material Issues and Catastrophic/Critical Risks Reporting to RHC

Material issues, such as changes in risk profiles, must be escalated promptly to RHC. Any new catastrophic or critical risks must be reported to RHC immediately, and to the local Board at the earliest opportunity.

## Principle 7 – Risks outside Group's Risk Appetite

In exceptional circumstances, it may be permissible to take on risks that would normally be outside the Groups risk appetite but this must be cleared in advance with the CEO, RHC.

## Principle 8 – Roles and Responsibilities of Internal Audit

Internal Audit is responsible for reviewing the risk profile and using this to develop audit plans that will confirm and verify the existence and effectiveness of managements mitigating controls.

## Principle 9 – Identifying, Assessing and Monitoring Risks

Methods for identifying, assessing and monitoring risks are detailed in MSIG Asia Risk Management Regulations and Guidelines and these should be read in conjunction with this Policy.

**Principle 10 – Reporting Risk Profiles**

1. The BPI/MS risk profile is to be reported quarterly to RHC, BPI Risk Management Office (RMO) and to the local Board of Directors using the standard report.

2. This report must include the risk map which shows residual impact and probability of occurrence of the key risks facing BPI/MS.

# 3. Exceptions

3.1 There are no exceptions to this Policy.

# 4. Non Compliance with Policy

4.1 Where BPI/MS is unable to comply with specific requirements with the policy, policy owner may apply to the Policy Owner in RHC for dispensation.

4.2 Reasons for requesting dispensation must be given in writing.

4.3 All such applications will be considered on their merits.

4.4 Written dispensation may be given on a permanent basis, or on a transitional basis.

# 5. Policy Owner

Masayuki Takahashi

# 6. Policy Manager

Merlina P. Mendoza

BPI / MS Insurance Corporation

A joint venture of Bank of the Philippine Islands and Mitsui Sumitomo Insurance

# BPI/MS

# Risk Management Regulations and Guidelines

ENDORSED BY:

| | | |
|---|---|---|
| MASAYUKI TAKHASHI | KOICHIRO KAWASAKI | MA. PERPETUA A. CUTIONGCO |
| YASUHIRO KANO | ANTHONY LOU M. BERNABE | NESTOR MAURICE JR. C. DANTES |
| ALBERTO C. SANTOS JR. | DANIELLE MARIA SALES-TORT | MERLINA P. MENDOZA |

# The Regulations

## Version 3.0

# Regulation No.1 – Risk Management Practices – Roles and Responsibilities

1. **Line Management**

    1.1 BPI/MS Management is ultimately responsible for the effective identification, management, monitoring and reporting of risks to RHC and to their local Board.

2. **Risk Manager**

    2.1 BPI/MS Management should appoint specialist risk managers who will assist them in discharging their responsibilities.

    2.2 They will provide support and independent challenge on the completeness, accuracy and consistency of risk assessments, and adequacy of mitigating action plans.

    2.3 They will be the point of contact on Risk Management issues between RHC and BPI/MS.

    2.4 This may or may not be a full time position.

3. **Risk Management Committee**

    3.1 BPI/MS is recommended to form a Risk Management Committee, headed by the Risk Manager or a SMT member overseeing Risk Management, and comprising members from the main functional areas of BPI/MS.

    3.2 Internal Audit may only be represented on the Committee as an Observer.

    3.3 They may provide advice and consultancy but they may not make, or participate in, decisions regarding design of mitigating controls.

4. **Internal Audit**

    4.1 Internal Audit provides independent assurance to the BPI/MS Audit Committee on the effectiveness of the risk management framework and gives its opinion on the appropriateness of the control environment structure.

## Regulation No.2 – Operating Models – Top-Down & Bottom Up Process

1. BPI/MS should consider all risks it faces. In order to cover all significant risks comprehensively, BPI/MS should identify risks by referring to those risks as stated in the Risk Library (see refer to Appendix)

2. Risk identification should be through a "top-down" and "bottom-up" process. By this, it is recommended that:

    2.1 BPI/MS senior management team determine the risks that may hinder the achievement of their strategic business aims ("top-down");

    2.2 While the line managers determine the risks to key business activities within their own departments ("bottom-up").

3. The BPI/MS Risk Management Working Committee (RMWC) will co-ordinate these activities, offer advice and guidance in identifying risks and controls, and compile reports for RHC and the Board.

4. This will lead to a greater understanding and management of risk throughout BPI/MS, and ultimately throughout the Region.

## Regulation No.3 – Inherent and Residual Risk Assessments

1. Risks should be assessed at both the inherent and residual levels, which allow greater transparency over what risks are considered to be adequately controlled.

2. Inherent and residual risks should be assessed by impact and probability, using the risk assessment methodology in Regulation No. 4. The impact and probability scales are set out in section 4.2.

3. Inherent risk is:

    3.1 The risk before any controls or mitigating actions are put in place; *or*

    3.2 The risk if the controls and mitigating actions in place all fail.

    3.3 Inherent risk assessment is necessary so that management may identify the "raw" risks that BPI/MS is exposed to in order to enable them to maintain management focus on the most important controls, and by internal audit as the basis for planning independent assurance work to test the effectiveness of key controls.

4. Residual risk assessments enable the prioritization of risk management actions by line management, and are used in reporting both the impact and the probability of risks to RHC and the BPI/MS Audit Committee.

5. Residual risk is the risk remaining in BPI/MS after applying existing controls and other mitigating actions (e.g. transfers of risk). It measures the risk that the operation must carry.

## Regulation No.4 – Risk Assessment: Impact and Probability Classification

4.2

1. **Overall Approach to Risk Assessment**

1.1 A common approach to determining the relative scale of issues, in terms of both impact and probability, and for the reporting of risks and audit issues is important in enable RHC to monitor risk within each operating unit on a consistent basis.

1.2 This also enables Internal Audit to plan their audits on a risk-based approach, relative to the BPI/MS' materiality.

1.3 Such consistency allows BPI/MS management to confidently prioritize risk and issues, and facilitates reporting to RHC.

2. **Materiality Thresholds**

2.1 Setting materiality thresholds requires judgment and cannot be based on a mathematical calculation alone, as this is unlikely to result in appropriate thresholds.

2.2 RHC will liaise with BPI/MS to ensure that materiality thresholds are in line with Group thresholds.

3. **Risk Measurement**

3.1 Risks are measured according to the probability and adverse impact of the event concerned, and are assessed on both an inherent and residual basis.

3.2 Reporting to RHC is based on residual risk levels. This ensures that management actions are concentrated on the maximum risk areas.

3.3 Risks are to be assessed using the following scales for impact and probability:

| **IMPACT** | **PROBABILITY** |
|---|---|
| Catastrophic | Extremely remote |
| Critical | Remote |

| | |
|---|---|
| Significant | Possible |
| Important | Likely to happen |

## 4. Risk Rating Table

4.1 The level of risk of each identified risk can be further rated as 'Low', 'Medium' or 'High' in accordance to the Risk Rating Table.

4.2 In the matrix below, the Risk Rating Table shows the combinations of both impact and probability risk scales.

| Impact | | | | |
|---|---|---|---|---|
| Catastrophic | Medium | High | High | High |
| Critical | Medium | Medium | Medium | High |
| Significant | Low | Low | Medium | Medium |
| Important | Low | Low | Low | Medium |
| | Extremely Remote | Remote | Possible | Likely to Happen |
| | Probability | | | |

## 5. Financial, Operational and Reputational impact criteria

In order to assess the impact of a risk, the consequences – actual or potential, this should be assessed on financial, operational and reputational criteria.

5.1 Financial

The risk results in a measurable loss of profit reflected in the BU's net profit.

This could be through:

- An actual operating loss, or
- A failure to maximise the benefit from an opportunity, or
- From the loss of an asset (including cash or information assets), or
- Any combination of the above.

5.2 Operational

The risk leads to an operational failure, including management failure, and BPI/MS fails to:

- Provide a quality service to its customers, or
- Run its business, or
- Maintain proper records, or
- Comply with laws, regulations, or policies and procedures; or
- Any combination of the above.

5.3 Reputational

- The risk has an adverse effect on the external reputation of the BPI and MSI Group.
- This may be through negative publicity in the media, or from negative comment and feedback from customers and intermediaries, or from the regulator.

## 6. Definitions of the 4 Impact categories

### 6.1 Catastrophic

- Financial: A serious threat to the viability of BPI/MS (e.g. 50% or more underachieving against operating profit), with the potential to cause the BU to cease operation.
- Operational: Irrevocable impact on BPI/MS operational performance.
- Reputational: Irretrievable damage to the BPI/MS reputation or brand, leading to a total loss of confidence by customers and intermediaries in MSI.

### 6.2 Critical

- Financial: A serious threat to the financial condition of BPI/MS or a serious threat of failing to materially achieve its performance targets (e.g. 5% or more underachieving against operating profit).
- Operational: Major impact on BPI/MS' operational performance.
- Reputational: Major damage to the BPI/MS' reputation or brand which might be long lasting and / or difficult to overcome.

### 6.3 Significant

- Financial: Substantial effect on BPI/MS but on its own would not threaten either the financial condition of the company or achievement of its performance targets.
- Operational: Issue would require careful management with some damage at an individual customer / stakeholder level E.g. An operational failure affecting 5% - 25% of BPI/MS customers
- Reputational: Issue would require careful management with some damage at an individual customer / stakeholder level.

### 6.4 Important

- Financial: Minor financial impact at BPI/MS level but will not materially affect company results. Typically an emerging issue or a higher risk issue mitigated down by controls.
- Operational: Issue is noticeable but easily manageable.
- Reputational: Issue is noticeable but easily manageable.

## 7. Selecting the appropriate impact category

7.1 Where a risk has a mixture of financial, operational and / or reputational consequences, the reported impact should be determined according to the highest impact arising from these criteria. For example, if a Disaster Recovery Plan failure would meet the criteria for a "critical" issue, but this incidence would result in a "catastrophic" outcome in terms of reputational damage, then the appropriate risk impact should be "catastrophic".

7.2 In most cases the selection of the appropriate impact category will involve the BU management team's judgment.

7.3 In more difficult cases, BPI/MS should consult with RHC.

## 8. Definitions of the 4 Probability categories

8.1 The probability of a risk occurring is measured on the following scale, where the probabilities and likelihood of events are meant as guidelines

Probability of occurrence

| In 12 months | Event likelihood | |
|---|---|---|
| Extremely remote | 1% | 1 in 100 year event |
| Remote | 4% | 1 in 25 years |
| Possible | 10% | 1 in 10 years |
| Likely | > 50% | within next 12 months |

8.2 Probability levels should be assessed according to the probability of the residual impact assessment occurring, and not of the related event occurring.

8.3 For example, where there is a risk of inadequate reserving due to an adverse weather event, say flooding, the assessment should take into account:

a. The likelihood of a material adverse weather event – in a number of territories such adverse events can occur more than once in a year, and

b. The quality of the reserving controls and risk mitigation (in the form of reinsurance) that reduce this risk.

8.4 As a result of the assessment of both of these factors, and assuming that the controls are operating effectively, we would normally expect BPI/MS to report that the risk of inadequate reserving giving rise to a "critical" residual risk is "remote" or even "extremely remote".

# Regulation No.5 – Risk Escalation Procedures for Deteriorated New or Emerging Risks

1. All new "catastrophic" and "critical" risks and control issues at BPI/MS materiality should be escalated to RHC immediately, as per the Policy.

2. Escalation should take place as follows:

   2.1 Clarify the residual impact of the issue:

   The relevant local Head of Department, Head of Audit and BPI/MS Risk Manager, where applicable, should discuss the risk or control issue and agree its potential residual impact at BPI/MS materiality.

   2.2 Escalate to RHC

   - Where the risk or issue is either "catastrophic" or "critical" it should be escalated to RHC immediately, in practice within 1-2 days depending upon the severity of the risk.
   - The BPI/MS President should escalate to the Regional Compliance Manager, RHC, who will then be responsible for further escalation within RHC and ultimately to Head Office if necessary.
   - Immediately after the risk or issue has been identified, there is likely to be action taken by BPI/MS to investigate it further, rather than to resolve the matter.
   - Escalation to RHC must not be delayed because an appropriate response has yet to be agreed within BPI/MS.

   2.3 Escalate to the BPI/MS Senior Management Team

   2.3.1 The process for escalating the issue within BPI/MS should be determined by the company.

   2.3.2 This is normally undertaken by either:

   - BPI/MS Group Head responsible for the business area within which the issue has arisen; or
   - BPI/MS CFO; or
   - BPI/MS President.

3. Information to escalate to RHC must include:

   3.1 Reason(s) why the risk or audit issue has been assessed as "catastrophic" or "critical" at BPI/MS materiality, and
   3.2 Actions being taken to address the matter.

4. Escalation to BU Board and Audit Committee:

4.1 In addition to the steps set out above, the BPI/MS Group Head must escalate any new "catastrophic" risks to its Board and Audit Committee at the next appropriate meeting.

## Regulation No.6 – Quarterly Reporting to RHC

1. **Risk Register**

1.1 Risk Register is a tool for the management of identified individual risks such as "claims", "underwriting", as well as specific risks such as "solvency" and "integration risk". It is important that risks are to be registered through appropriate process of identification and assessment. In addition to being international best practice, it is a requirement of the Japanese FSA that all risks have been considered, and they will look for evidence of this when conducting their reviews.

1.2 Accordingly, there should be a "Risk Register" (please refer to Appendix for a template sample) showing all risks and a brief explanation of the key controls mitigating those risks, along with the risk owner. This register should be presented so that the top 12 – 15 risks are the key risks that face BPI/MS and shows what risks management are primarily concerned with managing.

1.3 The register should be reviewed and updated at least bi-annually: many risks may not change significantly over time, but BPI/MS management will be expected to show evidence of review, i.e. minutes of Risk Management Working Committee meetings, discussion of risk as an agenda item on Senior Management Team meetings, etc.

2. **Key Risks (or "Bubble Map")**

2.1 The key risks identified within the Risk Register should be reported in a two dimensional graph which shows residual impact and probability.

2.2 The Residual Risk Map or Bubble Map (please refer to Appendix) shows each key risk as a 'bubble'. Each key risk is also supported by a more detailed written description of the risk in the Risk Profile Report. (please refer to Appendix) This includes:

2.2.1 Explanation of the risk, including rationale for the impact category.

2.2.2 Probability of the risk occurring, including rationale for the probability category

2.2.3 Current controls

2.2.4 Future mitigating actions. These must show who is responsible for the actions, and the implementation date. BPI/MS may include the names of other key staff involved in a particular project for their own management purposes, but it must be clear who the owner is – who is "in charge" of the action.

2.2.5 Where the implementation date has been passed, BPI/MS must provide an explanation of why the date was not achieved, and what actions will be taken to ensure that any new date stated will be achieved.

2.2.6 Risk acceptability.

2.2.7 Expected risk level on completion of the documented future mitigating actions

2.2.8 Target risk level and date by when the target level will be achieved

2.2.9 Business area(s) affected

2.2.10 BPI/MS senior manager accountable – the risk owner. This will normally only be one person.

2.2.11 Financial impact where it is possible to estimate, and appropriate

2.2.12 Key Risk Indicators (KRIs) and Key Control Indicators (KCIs) where appropriate (please refer to Appendix for more details on KRIs and KCIs )

3. The risk report should be comprehensive and include all material risks reported under the Group Policy set. For example it should include risks reported within Financial Condition Reports and the specialist risk profiles such as the IT or Compliance risk profiles. In practice the risks reported in these specialist risk profiles are summarized to a higher level for inclusion in the BPI/MS Risk Map, with the supporting detail available for reference.

4. The BPI/MS risk map must be agreed with the relevant BPI/MS risk owner or manager(s) prior to submission to RHC.

# Regulation No.7 – Risk Appetite

1. **Determining the acceptable level of an individual risk**

The risk appetite of the Group, and by BPI/MS, is set by the appropriate Board of Directors.

The acceptable level of risk for an individual risk, i.e. BPI/MS risk appetite, is determined through a combination of the following approaches:

1.1 Use the Group policies and guidance to provide clear 'rules' or 'minimum standards' and thereby define the acceptable risk level for the BU. These should be supplemented by BPI/MS policies and guidance.

1.2 Request the Board for guidance on the level of acceptability for a specific risk.

1.3 Request RHC for guidance on the level of acceptability for a specific risk.

1.4 Use the BPI/MS risk report to set out (for risks currently outside of appetite) the target risk that the BPI/MS senior management team considers 'acceptable' and the key mitigating actions that should achieve this target level by the stated date.

2. **Comparison to Risk Appetite for individual risks (Risk Acceptability)**

2.1 Each risk on the BPI/MS' Risk Profile should be compared with the risk appetite of the business for this risk.

2.2 The color of the risk 'bubble' in the risk map shows if the risk is within risk appetite, or if it is on track to return to within risk appetite by using one of the following 4 categories:

Green: Acceptable Risks

Sufficient controls are in place; and
The residual risks are within acceptable tolerance levels.

Amber: Mitigated Risks

These are outside of appetite, but which have future mitigating action plans that:
Reduce the risk sufficiently; and
Reduce the risk quickly enough.

Red-Amber: Volatile risks

These are Amber or Green risks where:

The risk is volatile due to external events which could result in the impact increasing rapidly; and
Existing mitigating controls or future actions are appropriate but will need to be reviewed frequently.

Red: Unacceptable Risks

These risks are unacceptable due to:
Insufficient mitigating action plans; or
Action plans that do not reduce the risk quickly enough.

3. **Adequacy of Risk Mitigating Controls and Future actions**

3.1 Each risk on the BPI/MS risk profile should be compared with the risk appetite of the business for this risk, taking into account the cost effectiveness of alternative risk mitigating options.

3.2 Where the risk is outside of appetite, the risk mitigation activities should be closely monitored.

3.3 The local management team is responsible for providing advice to the Board on whether or not:

a. The current controls are sufficient to manage the risk to within an acceptable level; and
b. The future actions that further mitigate the risk are sufficient to reduce the risk to an acceptable level, within an acceptable timeframe.

3.4 Where a risk mitigating activity falls behind schedule, a reassessment of the timeliness of actions in bringing the risk to within appetite must be made.

3.5 If the speed of delivery of the actions is unacceptable, a reassessment to 'Red' status must be made.

3.6 The implementation and testing of these controls is the responsibility of management within the business. Risk Managers should provide support and independent challenge on the adequacy of future plans and mitigating action plans before they table the risk report to the Risk Management Working Committee. Where material, the effectiveness and adequacy of these controls will be tested as part of the assurance program undertaken by the internal audit functions.

# Regulation No.8 – Integration Risk Assessment & Risk Profiling

1. **Role of Integration Steering Committee**

1.1 During an integration, a steering committee (ISC) would normally be established by the Board or local management to ensure smooth implementation.

1.2 It is recommended ISC scope should include reviewing and monitoring the integration risks identified including the action plans to mitigate these risks on a regular basis.

1.3 If necessary ISC should issue instructions or take decisions to ensure all identified risks are promptly followed up, remediated or mitigated.

1.4 If an ISC is not established, this role should be assumed by the Risk Management Working Committee and Senior Management Committee whichever is more appropriate.

1.5 It is the roles of local divisional/departmental workgroups or task forces set up to identify their respective integration risks and mitigation action plans.

1.6 The integration risks and mitigation action plans should be reported in BPI/MS Risk Register and discussed at the Risk Management Working Committee.

1.7 If necessary these risks should be escalated to BPI/MS Risk Profile so that they can be tabled for information, discussion and if necessary decision at local Board meetings.

1.8 All draft integration risks/profile and their mitigation action plans should be submitted to RHC Risk Management team for review and comments as part of regional Governance and Oversight functions before they are tabled at Board meetings.

1.9 Any decisions to be taken shall be made by local Board and/or CEO after taking into consideration RHC Risk Management team feedback.

1.10 RHC Risk Management will ensure relevant stakeholders or departments are consulted in BPI/MS and/or RHC before rendering feedback including suggestions.

## Regulation and Guideline Owner

N/A

## Regulation and Guideline Manager

N/A

# The Guidelines

## Version 3.0

# Guidance Note No.1 – Reference to MSIJ Policy

This policy should be read in conjunction with it:

1. MSIJ Risk Management Policy & Guidelines for Overseas Operations.
2. BPI General Policy on Operational and IT Risk Management

# Guidance Note No 2 – Reference to other MSIG Asia Regional Polices

The following are some of the policies which rely upon material within MSIJ Risk Management Policy and Guidelines for Overseas Operations, and should be read in conjunction with it:

**A-2 Compliance Policy**

This policy sets out an effective compliance and regulatory risk framework covering accountabilities, reporting and controls.

**A-5 Internal Audit Policy**

This policy defines the Group's process for providing objective, reliable audit assurance to the Group Board that the Group's internal controls and processes are operating effectively.

**A-6 Internal Controls Policy**

This policy sets out the principles to be adopted to ensure there is a consistent approach to internal controls within the Group.

**A-8 Legal Risk and Use of Lawyers Policy**

This policy sets out the principles and practices for the management of legal risks.

**B-1 Financial Management Policy**

This policy sets out the principles and practices for the financial management in the Group.

**B-2 Investment Policy**

This policy sets out the principles and practices for the management of investment risks.

**B-5 Taxation Policy**

This policy sets out the principles and practices for the management of tax risks.

**D-1 IT Governance Policy**

This policy sets out the principles and practices for the management of IT risks.

# Appendix

## Version 3.0

# Appendix 1 – Business Unit Covered under the Policy

1. BPI/MS INSURANCE CORPORATION

# Appendix 2 – Subsidiaries under BU Purview Covered

1. Not Applicable

# Appendix 3 – 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. | |

| | |
|---|---|
| RHC Policy Owner | |
| Dispensation granted? | YES / NO |
| Permanent or transitional? | PERMANENT / TRANSITIONAL |
| Additional comments or explanation by RHC | |
| Date this dispensation expires (if any) | |

**Notes for completion**

Be as specific and detailed as possible in requesting dispensation: help the RHC 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 maybe supplied under separate cover.

**MSIG Holdings (Asia) Pte Ltd**
**Regional Holding Company**
**April 2013**

# Appendix 4 – Financial Materiality Thresholds for Individual Business Units

These thresholds may be amended from time to time by RHC.

It is extremely important that both management and risk teams consider the non-financial criteria for assessing risks, as well as these financial criteria. This is because these non-financial criteria are often the main driver for a risk assessment, as they give rise to a higher risk assessment than the financial assessment alone.

For example:

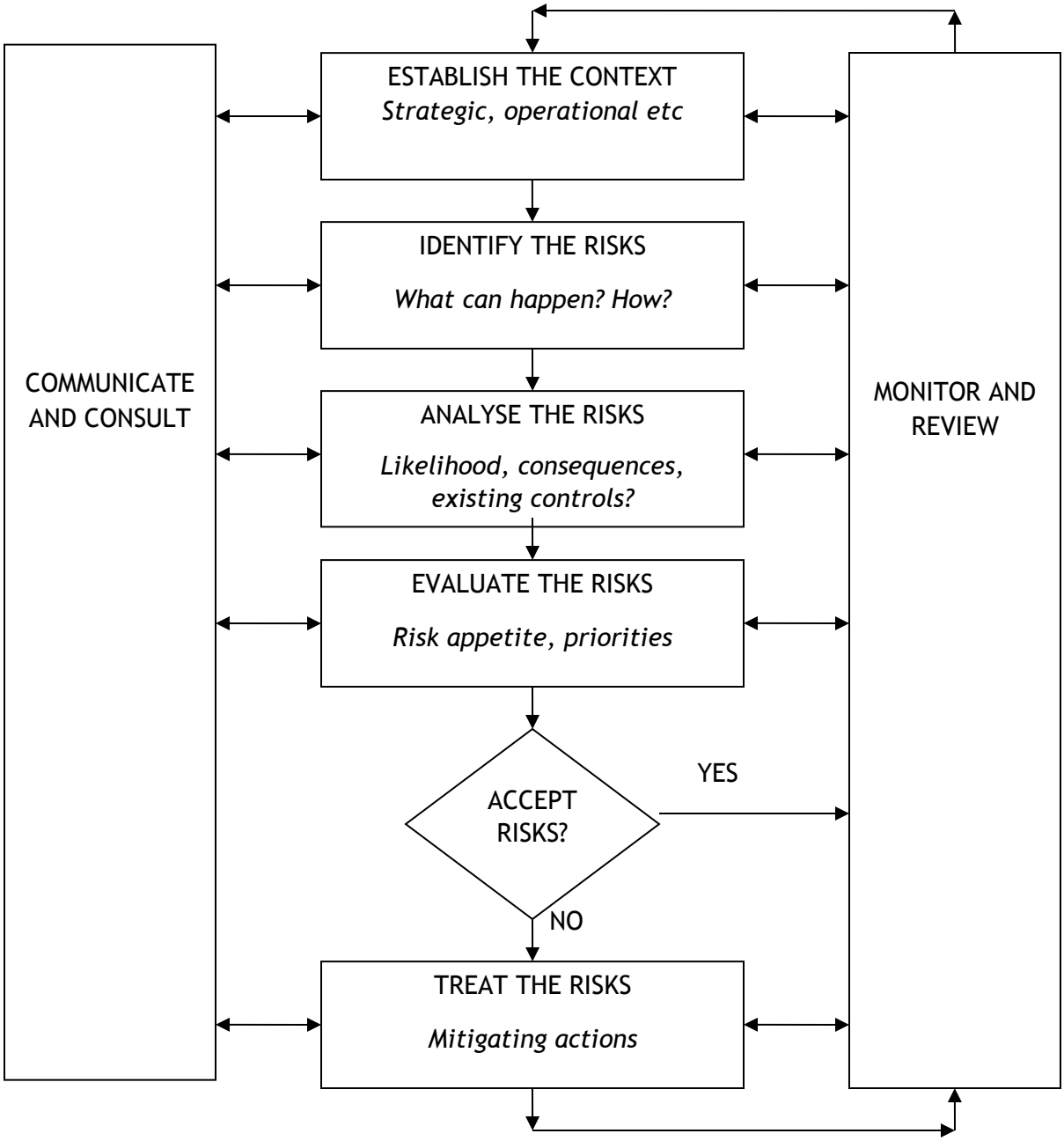
BU materiality levels (SGD millions)

| Catastrophic | Critical | Significant | Important |
|---|---|---|---|
| > 60 million | 60 to 15 million | 15 to 5 million | < 5 million |

For smaller scale BUs, these points may be considered:

- Financial loss that will bring the company to technical insolvency (below minimum solvency requirement but not necessarily real insolvent) should be considered as 'Critical'
- 5% of normalised Profit before Tax or 0.5% of Total Assets (excluding goodwill), whichever is higher should be considered as 'Significant'
- In the between, the scale should be based on management's risk appetite.

# Appendix 5 – Review Process Diagram



# Appendix 6 – Examples of Risk to be Included within each Risk Category

| | CATASTROPHIC | CRITICAL | SIGNIFICANT | IMPORTANT |
|---|---|---|---|---|
| **Financial** | **A serious threat to the viability of the BU**<br>• Equity market crash to levels that impact BU solvency requirements.<br>• Fundamental deterioration of back-year reserves giving rise to solvency issues.<br>• Catastrophe or terrorist act of an unforeseen size or type, not covered by the reinsurance programme. | **A serious threat to the financial condition of the BU or a serious threat of failing to materially achieve BU performance targets.**<br>• 5% or more underachieving against plan<br>• X% impact on a balance sheet item | **Substantial effect on the BU but on its own would not threaten either the financial condition of the BU or achievement of BU performance targets**<br>• Less than 5% underachieving against plan<br>• X% impact on a balance sheet item | **Minor impact from a financial perspective at BU level but will not materially affect BU results.**<br>• Typically an emerging issue or a higher risk issue mitigated down by controls. |
| **Operational** | **Irrevocable impact on the BU's or the Group's operational performance.**<br>• Operational failure affecting 50% or more of BU customers.<br>• Major disaster (e.g. bomb, flood, plane crash or sabotage) at a key IT processing centre for the BU that is a single point of failure with no recovery plan for such a disaster.<br>• Failure to achieve several key BU performance targets | **Major impact on the BU's or Group's operational performance.**<br>• Operational failure affecting 25-50% of BU customers.<br>• Failure of a key processing system that is likely to result in a failure to recover in more than 36 hours.<br>• A prolonged (1 week or more) network failure.<br>• Total failure or loss of a major BU third party (e.g. reinsurer or outsourcing provider).<br>• Failure to achieve a key BU business objective.<br>• An accumulation of a high number of uncleared | **Issue which would require careful management with some damage at an individual customer / stakeholder level.**<br>• Operational failure affecting 5 to 25% of BU customers.<br>• Failure of a key BU processing system.<br>• Partial failure of a major BU third party (e.g. reinsurer or outsourced provider).<br>• Total failure of a significant BU Corporate Partner.<br>• Disruption to one or more planned BU business objectives.<br>• Excessive claims leakage.<br>• Major failing in pricing processes, | **Issue is noticeable but easily manageable.**<br>• Operational failure affecting up to 5% of the BU customers.<br>• Deteriorating performance of a BU third party.<br>• Failure to recover an important BU system in less than 5 days.<br>• Frauds perpetrated against the BU, whether claims frauds or other types |

| | | | | |
|---|---|---|---|---|
| | | significant audit and/or risk issues | not picked up from MI. | |
| | **CATASTROPHIC** | **CRITICAL** | **SIGNIFICANT** | **IMPORTANT** |
| **Reputational** | **Irretrievable damage to the BU's or the Group's reputation or brand.**<br>• Downgrade of Mitsui Sumitomo Insurance Co., Ltd. credit rating to junk bond status by an external rating agency.<br>• Accounting/governance failures similar to those at Barings/Enron/Worldcom (i.e. issues are of such a magnitude that the BU is at risk of failing).<br>• Management failure at a BU executive level.<br>• Withdrawal of a key regulatory license. | **Major impact on the BU's or Group's reputation or brand which might be long lasting and / or difficult to overcome**<br>• Significant downgrade of Mitsui Sumitomo Insurance Co., Ltd. credit rating by an external rating agency<br>• Accounting /governance failings that are sufficiently serious to impart significant damage, but overall the BU is likely to be continuing.)<br>• Regulatory breach leading to regulatory restrictions being placed on the BU;<br>• Significant regulatory breach resulting in major public censure and/or extensive remediation programs at the BU. | **Issue which would require careful management with some damage at an individual customer / stakeholder level.**<br>• One point downgrade of Mitsui Sumitomo Insurance Co., Ltd. credit rating by an external rating agency.<br>• Management failure at a senior management level within a major BU.<br>• Significant adverse comment re the BU in national press, or equivalent.<br>• Any significant regulatory breach of regulations enforced by an "active" regulator, such as the BNM or MAS, with a record of imposing adverse penalties | **Issue is noticeable but easily manageable.**<br>• Adverse comment in local press<br>• Less significant regulatory breaches of regulations enforced by a less "active" regulator with no track record of imposing adverse penalties (fines, public censure or remediation programmes). |

# Appendix 7 – Guidance on making the Impact Assessment

A BU must assess the impact of its risks in order to support their escalation and prioritisation. This does not require scientific or mathematical risk measurement techniques, however to be effective, impact assessments need to be made in a meaningful and consistent way across all risks.

Financial measurement is complicated as there are different methods for calculating profits e.g. pre-tax, post-tax, including investment income, etc. Therefore, it will often be more appropriate to use the Operational or Reputational criteria for selecting the appropriate impact category.

1. **Operating profit vs alternative financial measures**

   The assessment of risks by financial impact, should be by reference to the impact on shareholders' funds.

   The financial measure for impact on shareholders' funds is operating profit as this tends to be the simpler measurement and is the value that most investors are interested in. Alternative measures of financial assessment will continue to be considered, in consultation with BUs.

2. **Converting alternative financial measures to an equivalent operating profit measure**

   A disadvantage of using profit as a measure is that a risk may not technically impact the Profit and Loss Account (P&L). For example, asset devaluations are made direct to reserves and do not pass through the P&L.

   Although this seems a fairly technical difference; in practice it is sufficient to treat such items as if they did impact on operating profit, but make the position clear in the risk narrative.

   Solvency and capital are key issues for insurance companies. To enable comparison with other reported risks, BUs should assess solvency or capital risks in terms of the affect they have on operating profit (i.e. the cost of capital), not the effect on capital itself. Where risks impact across a number of years, the most appropriate measure may be the net present value of the potential impact on the stream of future earnings.

   The measurement basis should be included in the risk description.

3. **One off loss vs. ongoing annual loss**

   Consideration of time-scales is an important issue for sizing and prioritising risks. It is important to use the same time frame when measuring risks as otherwise it is difficult to compare and rank them.

   The most appropriate period of measurement is a rolling period of one year, as this is a time-scale over which any potential risks should be reasonably foreseeable, and which

fits into the Financial Reporting calendar and Corporate Governance requirements on Group reporting.

However, BUs may also need to measure risks in the medium and long-term (say 3-5 years), so as to give early warning of new and emerging risks appearing on the horizon. Where such risks span a number of years, an annualised amount should be calculated in order to make it comparable with other reported risks. As there will be both short and medium/long term scenarios for risk issues, BUs should use the greater of 1 year's or 3–5 years' (annualised) effect on planned operating profit.

# Appendix 8 – Key Risk Indicators (KRIs) and Key Control Indicators (KCIs)

1. **Definition**

A KRI is a quantitative indicator for monitoring changes and risk control status.
KRI helps us to monitor our changing risk profile within our tolerance level.

The KRIs chosen will depend on what are the most appropriate indicators for the risk and the likely causes, as well as data available (i.e. exposure, management or results indictors)

Exposure Indicators are indicators for the status or changes of exposure
(e.g. 1. Maximum credit balance of single firm or person,
2. Risk amount by risk category,
3. Insured amount of natural catastrophe risk)

Management Indicators are indicators of the status which show the risk trend to be materialized
(e.g. 1. Average share prices,
2. Foreign exchange rates)

Result Indicators are indicators such as changes in number of materialized risks or amount of loss which help in recognising probability of unanticipated risk materialization (scale or number)
(e.g. 1. loss ratio,
2. Number of claims,
3. Number of Dishonest and Unlawful Acts)

The KRI should be such that:

i. it can be measured, i.e. a figure, a percentage, a rating, etc;
ii. each KRI has a *reasonable* pre-defined limit that triggers a reassessment of the risk. If the limits are too tight it will always be flagged and if too loose it will never trigger; and
iii. they are built around existing Key Performance Indicators (KPIs).

Different risks may require a variety of KRIs, but as a guide it is useful to aim for two to four KRIs for each risk.

A KCI is an indicator for monitoring the implementation status towards the goal of risk mitigation measures. KCI helps us to ascertain if we are 'in control' and if our controls are effective.

The KCIs chosen should be the primary key controls amongst all the risk mitigation plans. The goals (objectives and dues) of the primary key controls should be clarified so that implementation status can be monitored.
(e.g. 1. Observation status of categorised risk limits,
2. Implementation status of BCP drills)

Monitoring both KRIs and KCIs helps management to identify changing risk exposure and effectiveness of control measures.

They support the management of risk in the following ways:

i. As an early warning system of potential movements in risk;
ii. They are objective rather than subjective; and
iii. They show links or correlations between risks, where a KRI or a KCI is appropriate for two or more risks.

2. **KRI Trigger Levels**

Each KRI should be monitored against a set of triggers or risk tolerance levels. There are four trigger levels ranging from 1 (lowest) to 4 (highest).

| | |
|---|---|
| *1. Steady* | Monitored monthly by BU Risk Manager.<br>No further action required. |
| *2. Alert* | Monitored bi-weekly by BU Risk Manager.<br>Review Future Mitigating Actions and Current Controls |
| *3. SMT / Risk Management Working Committee Awareness* | Monitored weekly by Risk Manager.<br>Risk Management Working Committee informed,<br>Review Future Mitigating Actions and Current Controls |
| *4. Significant Change* | Change to probability / impact / appetite of the risk required, Risk Management Working Committee informed, KRIs to be reassessed |

3. **Example of the possible trigger levels for a KRI:**

If 'Staff turnover in Call Centre' was the KRI, the following may be the trigger levels:

| | |
|---|---|
| 1 Steady | Turnover of less than 1% |
| 2 Alert | Turnover between 1% and 5% |
| 3 SMT / RMWC | Turnover between 5% and 10% |
| 4 Significant Change | Turnover greater than 10% |

4. **Role of Risk Manager**

The risk manager will need to:

i. Agree trigger levels with management; and
ii. Monitor, review and challenge to ensure the right balance is found.

# Appendix 9 – High Level Risk Categories

(Please refer to Appendix – Risk Library for detailed descriptions on Risk Categories)

| | |
|---|---|
| **Business risk** | Risk of failure of the Board, or other body which has delegated authority from the Board, in its responsibility for:<br>• Understanding and approving the business plan (which includes strategy and policy statements) and the risk management systems.<br>• Ensuring the policies adequately reflect strategy and the systems provide a basis for the control of risks and commitments accepted by the company. |
| **Financial risk** | Risk arising from balance sheet mismanagement e.g. mismatch asset liability etc. This also includes non-compliance in taxation regulations. |
| **Insurance risk** | Risk includes underwriting, claim management and reinsurance. This may due to inappropriate pricing or selection of insurance policies and that claims liabilities previously established prove to be deficient. |
| **Credit risk** | Risk of loss due to counterparty default. |
| **Liquidity risk** | Risk that there are insufficient liquid assets to meet cash flow requirements. |
| **Market risk** | Risk of loss due to exposure to the movement in the level of financial variables such as equities, interest rates, or exchanges rates. |
| **Operational risk** | Risks of direct or indirect loss as a result of inadequate or failed internal processes, people or systems; or from external events. |
| **Group risk** | Risk of direct or indirect loss as a result of connection with a related undertaking. |

# Appendix 10 – Risk Library

Refer to attached.

A-3 Appendix 10 Risk Library

## Appendix 11 – Risk Register (Standard Template)

Refer to attached.

A-3 Appendix 11 Risk Register

## Appendix 12 – Risk Profile (Standard Template)

Refer to attached.

A3 Appendix 12 Risk Profile