GUIDELINE NO. TIU/G-3/2018/8

GUIDELINES ON RISK MANAGEMENT AND INTERNAL CONTROLS FOR INSURANCE COMPANIES AND TAKAFUL OPERATORS

1. INTRODUCTION

1.1. These Guidelines are issued pursuant to Section 88 of the Insurance Order, 2006 and section 90 of the Takaful Order, 2008 ("the Orders") to provide guidance, as part of its overall corporate governance framework, effective frameworks of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters and internal audit.

1.2. These Guidelines shall be read in conjunction with the following:

1.2.1. Insurance Order, 2006,

1.2.2. Takaful Order, 2008,

1.2.3. Notice on Corporate Governance for Insurance Companies and Takaful Operators [Notice No. TIU/N-3/2017/7],

1.2.4. Notice on Syariah Governance Framework for Financial Institution in Brunei Darussalam [Notice No. IFAU/N/1/2018],

1.2.5. Guidelines on Syariah Governance Framework for Financial Institution in Brunei Darussalam [Guidelines No. IFAU/G/2/2018],

1.2.6. Notice on the Application for Approval of Key Responsible Persons and Key Persons in Control Functions in Insurance and Takaful [Notice No. TIU/N-6/2017/10]; and

1.2.7. as well as any other notices, directives or guidelines, which the Authority may issue from time to time.

1.3. These Guidelines shall take effect on 1 January 2020.

2. DEFINITIONS

2.1. For the purpose of these Guidelines:

2.1.1. "Board" means the Board of Directors of the company;

2.1.2. “Concentration risk management” means any single (direct and/or indirect) exposure or group of exposures with the potential to produce losses large enough to threaten an insurer’s health or its ability to maintain its core business;

2.1.3. “Control functions” includes oversight functions where Senior Management has delegated some of its responsibilities for providing oversight of operational management including the Internal Audit, Risk Management, Compliance and Actuarial Functions;

2.1.4. “Insurer” means a registered insurance company under Insurance Order, 2006 and a registered takaful operator under Takaful Order, 2008, unless it is otherwise specified;

2.1.5. “Key Persons in Control Function” means a person who has responsibility independent from business lines to provide objective assessment, reporting and assurance on the effectiveness of an insurer’s policies and operations, and its compliance with legal and regulatory obligations. This includes persons who head the Financial, Risk Management, Compliance, Internal Audit and Actuarial functions.

2.1.6. “Operational risk” means a risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. For takaful undertaking, this also includes risk of loss resulting from Syariah non-compliance and failure in a takaful operator’s fiduciary responsibilities.

2.1.7. “Reinsurance” includes retakaful;

2.1.8. “Risk Appetite” is the aggregate level and types of risk an insurer is willing to assume, decided in advance and within its risk capacity, to achieve its business objectives and strategies.

2.1.9. “Senior Management” means persons having authority and responsibility for planning, directing and controlling the activities of the company as appointed by the Board, including the Principal Officer as defined in the Insurance Order, 2006 and Takaful Order, 2008.

3. RISK MANAGEMENT FRAMEWORK

3.1. The risk management framework is designed and operated at all levels of the insurer to allow for the identification, assessment, monitoring, mitigation and reporting of all risks of the insurer in a timely manner. Insurer should take into account the probability, potential impact and time horizon of risks.

3.2. The risk management framework should at least cover underwriting and reserving, asset-liability management, investments, liquidity and concentration risk management, operational risk management, conduct of business, reinsurance and other risk-mitigation techniques.

3.3. The risk management framework should be aligned with the insurer's risk culture and embedded into the various business areas and units with the aim of having the appropriate risk management practices and procedures embedded in the key operations and structures.

3.4. The risk management framework should include strategy and tools to mitigate against material risks, capturing both quantitative and qualitative elements of risks. For Takaful operators, the risk management approaches should be able to distinguish the different nature and combination of risks that are embedded within different types of Syariah contracts used to structure the products.

3.5. The risk management framework should also include a risk register serves as a risk profile report of the risks identified by the insurer, quantification where relevant, and the extent to which the risks have been managed and mitigated. The register should also include the interdependencies, wherever relevant, should be identified so that decisions on risk management are not taken in isolation.

3.6. Material changes to an insurer's risk management framework should be documented and subject to approval by the Board. The documents should be available to internal audit, external audit and the Authority for their respective assessments of the risk management framework.

3.7. Insurer, on a case by case basis as and when upon request by the Authority, should present their plan for remediation to the Authority if the framework is concluded to be deficient in the Authority's opinion and to report to it on the implementation of the plan.

4. RISK MANAGEMENT STRATEGY

4.1. An effective risk management framework should include a clearly defined and well documented risk management strategy approved by the Board with the following elements:

4.1.1. Includes a clearly defined risk appetite and takes into account the insurer's overall business strategy and its business activities (including any business activities which have been outsourced);

4.1.2. Objectives, key principles and proper allocation of responsibilities for dealing with risk across the business areas and business units of the insurer;

4.1.3. Any deviations from the risk management strategy or the risk appetite need to be approved by the Board;

4.1.4. Definition and categorisation of material risks (by type) to which the insurer is exposed including Syariah non-compliance risk, and the levels of acceptable risk limits for each type of these risk;

4.1.5. Process and tools for identifying, assessing, monitoring and reporting on risks;

4.1.6. Projected economic and market conditions including their impact on the risks inherent in the core activities;

4.1.7. Necessary modifications and improvements are identified and made in a timely manner; and

4.1.8. Role(s) of effective risk management functions.

4.2. An effective risk appetite statement should consider the existing risk profile, capacity and willingness to assume each risk in respect of each segregated part of the operation, as well as the insurer's attitude towards risks.

4.3. The risk management strategy should be reviewed periodically taking into account insurer's financial performance and market developments, especially when there are material changes to the insurer's operations or its business strategy.

4.4. When new business activities are being pursued, senior management should ensure that all key risks associated with the activities have been identified and assessed to determine whether these risks are within the insurer's risk appetite.

4.5. The risk management strategy should be translated into risk policies and procedures and effectively communicated to all relevant staff. The overall risk management policy of the insurer should outline how relevant and material risks are managed.

4.6. The insurer should establish a risk management function if warranted by the size, scale and complexity of its operations. This function would be primarily responsible for the development of and ensuring compliance with the insurer's risk management policies and procedures. The function may also be supported by actuarial expertise to assess the insurer's actuarial and financial risks.

5. RISK POLICIES AND PROCEDURES

5.1. Risk policies should set out the conditions and guidelines for the identification, acceptance, monitoring and management of risks. These policies should be well-defined and consistent with the insurer's risk strategy, as well as adequate for the nature and complexity of its activities including the specificities of the operating model and Syariah obligations in the case of takaful operators.

5.2. At a minimum, the risk policies should cover the following:

5.2.1. The identification, measurement and communication of key risks to the Board including the possibility of new risks emerging in the environment in which it does business, even though its business may not have changed;

5.2.2. The process by which the Board decides on the risk appetite, as well as the frequency of review of risk limits;

5.2.3. The roles and responsibilities of the respective units and staff involved in acceptance, monitoring and management of risks;

5.2.4. The approval structure for product development, pricing, underwriting, claims handling and reinsurance management, including authority to approve deviations and exceptions;

5.2.5. The principles and criteria relating to product development, pricing, underwriting, claims handling and reinsurance management;

5.2.6. The determination and approval of technical provisions to ensure that provisions are appropriately estimated and deficits; and

5.2.7. The management of concentration risk and exposures to catastrophic events, including limits, reinsurance, portfolio monitoring and stress testing.

5.3. The insurer should establish appropriate procedures and processes to implement its risk policies in the form of controls, checks and monitoring mechanisms. These should be documented and set out in sufficient detail to provide operational guidance to staff.

5.4. The insurer should have in place proper and effective reporting systems to satisfy the requirements of the Board with respect to reporting frequency. Level of detail, usefulness of information and recommendations to address issues of concern. There should be clear guidelines on the type of information to be reported to the Board on a regular basis as well as when certain information or development ought to be communicated immediately to the Board. The head of risk management function should have the authority and obligation to inform the Board promptly of any circumstance that may have material effect on the risk management framework of the insurer.

5.5. The reporting process should cover all internal and external risk reporting requirements, including how relevant and reliable risk information is capture at the appropriate level of detail for each level of user, including operational management, the risk management committee, the Board, the Syariah Advisory Body, and any required public or regulatory reporting.

6. RISK IDENTIFICATION, CONTROL AND MONITORING

6.1. An effective risk management process to address risks arising from core insurance activities; namely product development, pricing, underwriting, claims handling and reinsurance management should include the following:

6.1.1. Risk identification and measurement

An insurer should have effective means of obtaining pertinent information to identify and measure its exposure to risks inherent in its core activities. Where a risk is not readily quantifiable, for instance some operational risks, an insurance should undertake a qualitative assessment that is appropriate to the risk and sufficiently detailed so that it be useful for risk management.

Insurer should aim to identify key potential causes for operational failure of the operations, including failure in internal processes, possible negligent, incompetent or fraudulent activities of its internal human resources, and other failures of its systems.

6.1.2. Risk evaluation

The identified risks should be evaluated against insurer's risk appetite, and the insurer should decide on the priority to be assigned to address each of the risks and the appropriate responses.

6.1.3. Risk control and mitigation

The insurer should implement necessary measures to control and mitigate the identified risks. Risk control/mitigation measures include setting appropriate standards and limits that are clearly documented and assigning limits to relevant staff that are commensurate with the experience and competence of the respective individual.

6.1.4. Risk monitoring and review

There should be an effective monitoring system to track whether any risk indicators have been triggered, and to ensure that risk standards and limits are complied with as intended and any deviation is duly approved and documented. The insurer should also establish clear procedures to investigate such incidents from recurring. The consequences for non-compliance with established limits should be clear and pre-determined.

6.2. The outsourcing of any significant activity of an insurer requires appropriate definition, approval, monitoring and control to ensure that the risks associated with the outsourced activity are properly managed. If an activity is outsourced, the insurer needs to ensure that the terms on which it is outsourced have due regard to the compliance and control requirements of the operations. Outsourcing providers may be unfamiliar with those requirements, particularly those relating to Syariah for takaful operators.

6.3. Syariah non-compliance risk is an operational risk which requires processes and controls to prevent non-compliance and to detect and correct any instances that do occur.

7. INTERNAL CONTROLS FRAMEWORK

7.1. An insurer should establish and maintain an internal control framework that reflects the risk policies adopted. The purpose of an internal control framework is to provide assurance at all levels of management that business processes are being adhered to, and ultimately to enable the Board to determine that the undertaking is following the approved strategy and risk appetite, agreed policies and processes, and applicable laws and regulations.

7.2. The internal controls framework should ensure effective and efficient operations, adequate control of risks, prudent conduct of business, reliability of financial and non-financial information reported (both internally and externally), and compliance with laws, regulations, supervisory requirements and the insurer's internal rules and decisions.

7.3. The framework should be designed and operated to assist the Board and Senior Management in the fulfilment of their respective responsibilities for oversight and management of the insurer. It should cover all units and activities of the insurer and should be an integral part of the daily activities of an insurer. An effective framework requires an appropriate control structure with control activities defined at every business unit level.

7.4. An effective internal controls framework includes, at a minimum, the following:

7.4.1. Appropriate segregation of duties and controls to ensure such segregation is observed and conflicts of interest are prevented;

7.4.2. Appropriate controls for all key business processes and policies, including for major business decisions and transactions. These include policies on training in respect of controls for employees.

7.4.3. Appropriate controls to provide reasonable assurance over the accuracy and completeness of the insurer's books, records, and accounts and over financial consolidation and reporting, including the reporting made to the Authority;

7.4.4. Processes for regularly checking that the totality of all controls forms a coherent framework and that this framework works as intended; fits properly within the overall corporate governance structure of the insurer; and provides an element of risk control to complement the risk identification, risk assessment, and risk management activities of the insurer.

7.5. The Board should have an overall understanding of the control environment across the various entities and businesses, and require Senior Management to ensure that for each key business process and policy, and related risks and obligations, there is an appropriate control.

7.6. The Board should also ensure there is clear allocation of responsibilities within the insurer, with appropriate segregation, including in respect of the design, documentation, operation, monitoring and testing of internal controls. These responsibilities should be properly documented.

8. CONTROL FUNCTIONS

8.1. Insurers should have control functions as part of effective risk management and internal controls frameworks, including risk management, compliance, actuarial matters and internal audit (including Syariah risk management, compliance and audit for takaful operators). These functions add to the governance checks and

balances of the insurer and provide the necessary assurance to the Board in the fulfilment of its oversight duties. Nonetheless, this will depend on the scale, nature and complexity of the insurer's business.

8.2. The appointment, performance assessment, remuneration, discipline and dismissal of the head of control functions should be done with the approval of, or after consultation with, the Board or the relevant Board committee. The insurer should notify the Authority of the reasons for dismissals of heads of control functions.

8.3. Each control function should have the resources necessary and meet any applicable professional qualifications and standards to fulfil its responsibilities and achieve the specific goals in its areas of responsibility with higher expectations apply to the head of each control function. The head of each control function should review regularly the adequacy of the function's resources and request adjustments from Senior Management as necessary.

8.4. The Board should approve the authority and responsibilities of each control function to allow each control function to have the authority and independence necessary to be effective.

8.5. The Board should periodically assess the performance of each control function, which may be done by the full Board, by the Chair of the Board, by the relevant Board committee or by the Chair of the relevant Board committee.

8.6. Notwithstanding the possibility for insurers to combine certain control functions, a control function should be sufficiently independent from Senior Management and from other functions to allow its staff to:

8.6.1. Serve as a component of the insurer's checks and balances;

8.6.2. Provide an objective perspective on strategies, issues, and potential violations related to their areas of responsibility; and

8.6.3. Implement or oversee the implementation of corrective measures where necessary.

8.7. The Board should grant the head of each control function the authority and responsibility to report periodically to it or one of its committees. The head of each control function should also have the opportunity to communicate directly and to meet periodically with the Chair of any relevant Board committee and/or with the Chair of the full Board without management present.

Issue date: 6 Rabiulakhir 1440 / 14 December 2018