

Insurance (Risk Management) Rules 2016

INSURANCE ACT

FSC Rules made by the Financial Services Commission under section 130 of the Insurance Act and section 93 of the Financial Services Act

1. Citation

These rules may be cited as the **Insurance (Risk Management) Rules 2016**.

2. Interpretation

In these rules –

“Act” means the Insurance Act;

"affiliated corporation" means an entity or a legal arrangement which –

(a) in relation to another entity, stands as a parent or subsidiary of that entity;

(b) is a parent or subsidiary of an entity referred to in paragraph (a); or

(c) in relation to another entity, is a member of the same group of corporations by virtue of common ownership or control;

“Board” means the board of directors of an insurer;

“corporate event” means –

- (a) a merger, acquisition, joint venture, change in control or significant shareholdings or any similar event; or
- (b) any unplanned event significantly affecting the business plan of an insurer;

“group” means an insurer and all its affiliated corporations;

“MIS” means the management information system required to be maintained under rule 13;

“ORSA” means the own risk and solvency assessment required to be carried out under rule 10;

“risk appetite” means the level of risk an insurer is prepared to accept in pursuing its objectives, having regard to the interests of shareholders and policyholders;

“RAS” means the risk appetite statement required to be made under rule 7;

“risk management framework” or “RMF” means the totality of the strategies, systems, policies, processes, controls and human resources for identifying, assessing, monitoring, managing and reporting on all material risks, both internal and external, to which an insurer is exposed;

“risk officer” means the officer appointed by an insurer under rule 12;

“RMS” means the risk management strategy required to be implemented pursuant to rule 8;

“risk tolerance” means the limits that an insurer sets for the maximum level of individual risk beyond which the insurer is under an obligation to take action to maintain or restore its capital targets.

3. Risk Management Framework

- (1) An insurer shall set up and at all times maintain a RMF to enable it to effectively develop and implement strategies, policies, procedures and controls to manage the material risks described in the Schedule.
- (2) The RMF of an insurer shall be approved by its Board and shall include -
 - (a) a RAS;
 - (b) a RMS;
 - (c) the business plan referred to in rule 9;
 - (d) an ORSA;
 - (e) the liquidity policy referred to in rule 11;
 - (f) a designated risk management function; and
 - (g) a description of the responsibilities, roles and reporting lines within the insurer for the management of material risks.
- (3) An insurer shall submit all documentation relating to its RMF to the Commission not later than 6 months after each balance sheet date.
- (4) An insurer shall notify the Commission of any corporate event which require a reassessment of its RMF within 10 days of such event.
- (5) The reassessment referred to in paragraph (4) shall be completed by the insurer within 3 months of the date of the corporate event.
- (6) Where the RMF of an insurer is changed, the insurer shall submit its updated RMF to the Commission within 30 days of the date of the change.
- (7) No action shall lie against the Commission, any staff of the Commission, the Chief Executive or any member of the Board of the

Commission, for any damage or loss suffered as a result of the contents of any RMF filed with the Commission.

Amended by [GN 264 of 2020]

4. Materiality of risks

The RMF shall consider the materiality of the risks described in the Schedule in accordance with its nature, scale and complexity.

5. Responsibility for the Risk Management Framework

- (1) The Board shall be ultimately responsible for –
 - (a) the setting up of a RMF;
 - (b) overseeing the implementation and subsequent monitoring of the RMF;
 - (c) determining the risk culture of the insurer;
 - (d) providing management with leadership and guidance to achieve the desired risk culture;
 - (e) ensuring that any person responsible for risk management has appropriate skill, knowledge, independence and authority; and
 - (f) defining the roles and responsibilities of management in relation to risk management.
- (2) The Board may, where it thinks fit, set up a sub-committee referred to in section 38 of the Act with responsibility for risk management.
- (3) The Board shall ensure that the risk officer reviews and reports to the Board on compliance with these rules at least once a year.

- (4) The Board shall ensure that the auditor, appointed under section 40 of the Act, reviews and reports to the Board on compliance with these rules at least once a year.
- (5) The Board shall ensure that the actuary, appointed under section 40 of the Act, reviews and reports to the Board, on the effectiveness of the RMF at least once a year.
- (6) The reviews referred to in paragraphs (4) and (5) shall, as the case may be, assess whether the RMF of the insurer –
 - (a) is implemented and effective;
 - (b) is still appropriate, taking into account the insurer's current business plan;
 - (c) is consistent with the insurer's risk appetite;
 - (d) is supported by adequate resources; and
 - (e) accurately documents key elements of the insurer's strategy for managing risk.
- (7) A copy of the reports referred to in paragraph (4) and (5) shall be signed by the auditor or the actuary who make the review and shall be submitted by the insurer to the Commission not later than 6 months after each balance sheet date.
- (8) The Board shall ensure that the insurer reviews and updates its RMF, including its RAS and RMS, annually.
- (9) The management of an insurer shall be responsible for -
 - (a) the day to day management, decision making, identification, assessment, mitigation and monitoring of risks, including the maintenance of risk registers; and

- (b) the allocation of roles and responsibilities regarding risk management.

Amended by [GN 264 of 2020]

6. Enterprise Risk Management for Groups

- (1) An insurer that is part of a group shall consider, in its RMF, any material risk arising from all affiliated corporations.
- (2) Risks associated with affiliated corporations shall be identified, assessed and incorporated in the RMF, RAS and RMS.
- (3) Where an insurer is operating as a branch of a foreign company, these rules shall apply only to the risk management of the branch.
- (4) The insurer shall assess and record any linkage and difference between its RMF and the RMF of the group.
- (5) An insurer forming part of a group may adopt elements of the group RMF and control mechanisms, provided that the group RMF complies with these rules.

7. Risk Appetite Statement

- (1) The Board shall after considering all relevant risks determine the risk appetite for each material risk set out in the RMF.
- (2) The risk appetite including the qualitative and quantitative levels of each risk identified shall be described in a RAS.
- (3) The Board shall review the RAS annually and shall ensure that the insurer's business plan and strategies are consistent with the RAS.
- (4) The RAS shall, for each material risk, document the processes for –
 - (a) setting the risk tolerance levels;

- (b) monitoring compliance adherence with the risk tolerance levels;
 - (c) taking action where any risk tolerance level is breached; and
 - (d) the annual review under paragraph (3).
- (5) Any new business initiative during the course of a year shall be assessed by the insurer to ensure consistency with its risk tolerance levels.

8. Risk Management Strategy

- (1) An insurer shall implement a RMS which shall describe the insurer's strategy for managing risk and the implementation of key parts of the RMF.
- (2) The RMS shall include a description of –
 - (a) how the RMF is developed and embedded in the business plan;
 - (b) each material risk identified and how each identified material risk is to be managed including any policies and procedures;
 - (c) the risk management function including roles and responsibilities;
 - (d) how awareness of the RMF is promoted throughout the insurer and the group;
 - (e) how an appropriate risk culture is to be achieved; and
 - (f) the insurer's risk appetite.

9. Business Plan

- (1) An insurer shall maintain a three-year rolling business plan, incorporating financial forecasts for at least 3 years including the projected solvency position, which sets out the insurer's strategic objectives and how these are to be achieved.
- (2) The business plan shall -
 - (a) be reviewed and updated at least annually;
 - (b) identify the material risks associated with the strategic objectives and state how those risks are to be managed;
 - (c) be subjected to stress testing made in accordance with the insurer's RMF, RAS and RMS; and
 - (d) include the whole of the insurer's operations and any group strategy which may impact the insurer.

10. Own Risk and Solvency Assessment

- (1) An insurer shall develop and at all times maintain an ORSA process which shall include an assessment of -
 - (a) the overall financial resources necessary for managing its business based on its own risk tolerance levels and business plan and for meeting regulatory requirements; and
 - (b) the quality and adequacy of its capital resources to meet regulatory capital requirements and any additional capital needs.
- (2) An insurer shall carry out an ORSA at least once a year and shall review it at least on a quarterly basis to assess the adequacy of its risk management and its current and prospective solvency position.

11. Liquidity policy

- (1) An insurer shall develop and at all times maintain a liquidity policy approved by its Board to manage its material liquidity risks.
- (2) An insurer forming part of a group shall describe in its liquidity policy how its liquidity is segregated from the group.
- (3) The liquidity policy referred to in paragraph (1) shall consider the results from stress testing.

12. Risk Management Function

- (1) An insurer shall have a risk management function which shall –
 - (a) be responsible for assisting the Board, Board sub-committees and management in developing and maintaining the RMF;
 - (b) be commensurate with the nature, scale and complexity of the insurer;
 - (c) be resourced with staff who have clearly defined roles and responsibilities and who possess appropriate experience and qualifications to exercise those responsibilities; and
 - (d) cover all aspects of the insurer that have the potential to generate material risk, including information technology system and system development resources.
- (2) An insurer shall appoint a person of sufficiently senior status, suitably qualified and experienced as risk officer.
- (3) The risk officer referred to in paragraph (2) shall be fit and proper in accordance with the requirements of section 20 of the Financial Services Act.

- (4) No appointment of a risk officer shall take effect without the prior approval of the Commission.
- (5) The risk officer shall be responsible for the risk management function and shall have a direct reporting line to the Board or the relevant Board sub-committee and shall report to the Board any significant breach of, or material deviation from, the risk management framework.
- (6) The risk officer shall be independent from business lines, other revenue generating responsibilities and the finance function of the insurer.
- (7) Where the role of the risk officer is combined with any other management function, the insurer shall take measures to avoid conflict of interest and to manage any conflict.
- (8) The insurer may outsource its risk management function if appropriate to its nature, scale and complexity and shall forthwith notify the Commission of the outsourcing.

13. Management Information System

- (1) An insurer shall, at all times, maintain an adequate MIS to measure, assess and report on all material risks.
- (2) The MIS shall provide the Board with timely and accurate information on the insurer's risk profile.
- (3) The MIS shall include data collection analysis and reporting system which facilitates aggregation of exposures, risk measurement, reporting and stress testing.

14. Outsourcing

- (1) When delegating or outsourcing any function, an insurer shall ensure that the delegate is fit and proper and is able to meet the requirements of these rules.
- (2) An insurer shall not be discharged from its responsibilities upon any delegation or outsourcing arrangement and shall ensure compliance with all requirements of the relevant Acts.
- (3) Notwithstanding any delegation or outsourcing arrangement, an insurer shall ensure that all books and records of the service or transaction delegated or outsourced shall be made available for inspection by the Commission.
- (4) An insurer shall identify, assess, manage, mitigate and report on risks associated with outsourcing to ensure that it can meet its financial and service obligations.
- (5) Where an insurer outsources any function, it shall reassess its risk profile and determine whether additional control, monitoring or reporting is required.

15. Register

An insurer shall establish and at all times maintain a risk register which shall record –

- (a) all risks relevant to the insurer;
- (b) how the risks are managed; and
- (c) compliance and breach.

16. Commencement

- (1) Subject to paragraph (2), these rules shall come into operation on 1 July 2017.
- (2) Rule 12 shall come into operation on 1 January 2017.

(3) Made by the Financial Services Commission on 10 October 2016.

SCHEDULE
(rule 4)

| Risk | Description |
|---------------------|--|
| Business Continuity | The risk which arises from business disruption of an insurer and impairment of its ability to function properly and the assessment of backup plans that are in place, including but not limited to issues such as premises, data, systems, telephony or staffing. |
| Capital | The risk which arises from capital to support business plans, assessing solvency, the output of stress testing and future capital assessment. |
| Credit | The risk which arises from counterparties including reinsurers, investments and intermediaries holding premiums and the assessment of the financial strength of the counterparty and includes default risks, concentration risks and liquidity risks. |
| Group affiliation | The risk which arises from membership of a financial services group, including risk for an insurance group in respect of the widest group of which it is part and includes the risk that an insurer may be adversely affected by an occurrence (financial or non-financial) in another group entity. |
| Insurance | The risk which arises from the core insurance business and would include such matters as underwriting, claims management, pricing, reinsurance and product design. |
| Investment | The risk which arises from asset and liability matching, valuation, concentration, liquidity and the application of any provision relating to investments as set out in the relevant Acts. |
| Liquidity | The risk which arises from having insufficient liquid assets, including investments, to meet the obligations to policyholders such as paying claims, suppliers, intermediaries and operating expenses including staff remuneration. |
| Operational | The risk which arises from all aspects of running the business, including systems, processes, reporting, human resources, customer service, IT, data security and fraud management. |

| | |
|---------------------|---|
| Outsourcing | The risk which arises from outsourcing any function and which is inherent to that function and the controls, including the reporting mechanisms in place to monitor the outsourced function. |
| Reinsurance | The risk which arises from net retentions, catastrophe exposures, and exposures above the level of reinsurance protection, horizontal exposures as well as counterparty risk, credit risk and concentration risk. |
| Other material risk | Any other material risk arising out of the conduct of insurance business. |