South African Reserve Bank

Prudential Authority

*Text in **bold** and **underline** is an Insertion/Addition *Text with a ~~strike-through~~ is a Deletion

Prudential Standard GOI 3

Risk Management and Internal Controls for Insurers

Objectives and Key Requirements of this Prudential Standard

Effective risk management is fundamental to the prudent management of an insurer. This Standard requires insurers to have a board-approved enterprise-wide risk management system consisting of the following main components:

- *A risk management strategy for the insurer, including a risk appetite statement and associated risk limits for different types of material risks, activities, and business units;*
- *Risk management policies that address the material risks that arise from the insurer's business activities;*
- *Risk management procedures and tools that enable the insurer to identify, assess, monitor, report on, and mitigate the material risks to which it is exposed;*
- *An effective system of internal controls to ensure that the strategies, policies, and processes in the risk management system are in fact in place, being observed, and attaining their intended outcomes; and*
- *A risk governance structure including at least the following control functions: a risk management function, a compliance function, an internal audit function, and an actuarial function.*

Table of Contents

1. Application 2
2. Roles and Responsibilities 2
3. Commencement and Transition Provisions 2
4. Principles 2
5. Risk Management Strategy 3
6. Risk Management Policies 4
7. Risk Management Procedures and Tools 5
8. Internal Controls 5
9. Risk Governance - General Requirements for Control Functions 6
10. Risk Governance – Heads of Control Functions 7
11. Risk Management Function 8
12. The Compliance Function 9
13. The Internal Audit Function 9
14. The Actuarial Function 10

Attachment 1: Policies for Managing Financial Risks 12

1. Application

1.1. This Standard applies to all insurers licensed under the Insurance Act, 2017 (the Act), other than microinsurers, Lloyd's and branches of foreign reinsurers. The application of these Standards to insurance groups that have been designated as such by the Prudential Authority, under section 10 of the Act is addressed in a separate standard, GOG (Governance and Operational Standard for Groups).

1.2. Unless otherwise indicated, all references to "insurer" in this Standard can be read as a reference to life insurers, non-life insurers and reinsurers.

2. Roles and Responsibilities

2.1. An insurer's board of directors is ultimately responsible for ensuring that the insurer complies with the principles and requirements of this Standard, including establishing the insurer's overall risk appetite and ensuring the insurer has in place effective systems for risk management and internal control to address the key risks it faces.

2.2. The heads of the insurer's risk management, compliance and actuarial functions are responsible for providing input and expressing an opinion to the board of directors about the operations, efficiency and effectiveness of the components of the systems for risk management and internal controls relevant to their respective areas of responsibility.

2.3. An insurer's internal audit function or an objective external reviewer must regularly review the systems for risk management and internal controls and provide assurance to the board of directors that the systems are effective.

2.4. An insurer's auditor must provide assurance to the insurer and the Prudential Authority, if requested, that the insurer complies with the requirements of this Standard. The auditor must report to the board of directors and the Prudential Authority any matters identified during the performance of its responsibilities that are contrary to the Standard or a part thereof.

3. Commencement and Transition Provisions

3.1. This Standard commences on 1 July 2018.

Version Number	Commencement Date
1	1 July 2018
2	**1 December 2020 – as amended by Joint Standard 1 of 2020 – Fitness, propriety and other matters relating to significant owners**

4. Principles

4.1. Insurers are in the business of risk. Insurers absorb risks from the economy and manage them by pooling and hedging. Effective risk management is critical to an insurer being able to honour its promises to policyholders.

4.2. An insurer must have a board-approved, enterprise-wide risk management system, consisting of a risk management strategy, policies, and related procedures, and tools for assessing, monitoring, reporting, and mitigating material risks that may affect its ability to meet its obligations to policyholders.

4.3. The insurer's risk management strategy must include a risk appetite for the insurer. The insurer's risk appetite should be aligned with its risk management strategy and business plan / business objectives.

4.4. An insurer must establish, maintain and operate within a system of effective internal controls designed to ensure that the risk management system is operating effectively and there are appropriate checks and balances to ensure that the insurer operates effectively and efficiently.

4.5. To provide appropriate governance over the risk management system and system of internal controls, an insurer must establish and adequately resource at least the following control functions:

a) a risk management function;
b) a compliance function;
c) an internal audit function; and
d) an actuarial function.

5. Risk Management Strategy

5.1. An insurer's board-approved risk management strategy sets out the types of risks that the insurer is willing to retain in implementing its business plan, and the way in which it will manage those risks. Material risks that are central to an insurer's risk management strategy include the lines of insurance business the insurer plans to engage in, and the mix of insurance risks it is targeting.

5.2. An insurer's risk management strategy must have an enterprise-wide focus and address all sources of risk that may impact on the financial soundness of the insurer, not just insurance risks.

5.3. At a minimum, an insurer's documented risk management strategy must:

a) identify the objectives of the strategy;
b) describe each current material risk and emerging risks, and the insurer's approach to managing those risks;
c) list the policies and procedures for dealing with risk management;
d) summarise the roles and risk management responsibilities of the risk management function, the board of directors, board committees and senior management;
e) include a documented process for board approval for any deviations or changes from the risk management strategy or risk appetite; and
f) outline the insurer's approach to ensuring all persons within the insurer have awareness of the risk management system and for instilling an appropriate risk culture across the insurer.

5.4. An insurer's risk management strategy must be consistent with the nature, scale and complexity of its business.

5.5. An insurer's risk management strategy must include a clearly defined risk appetite statement, which quantifies the levels of different types of risk the insurer is willing to retain. The insurer's risk appetite must be consistent with its risk management strategy and business plan / business objectives.

5.6. At a minimum, an insurer's risk appetite statement must identify clearly:

a) the overall level of risk the insurer is prepared to accept in pursuit of its strategic objectives and business plan, giving due consideration to the interests of policyholders; and
b) for each type of material risk, the maximum level of risk that the insurer is willing to operate within, expressed as a limit based on its risk appetite, risk profile and capital strength.

5.7. Where risks are not readily quantified, the risk management strategy and risk appetite should set qualitative limits on risk.

5.8. The risk management strategy must be supported by processes with respect to the risk appetite statement for:

a) ensuring that risk limits are set at appropriate levels, based on an estimate of the impact of a breach of a risk limit, and the likelihood that each material risk is crystallised;
b) monitoring and reporting compliance with each risk limit and for taking appropriate action in the event that a particular limit is breached; and
c) review of the risk appetite and risk limits, and the timing thereof.

5.9. An insurer's risk management strategy must be reviewed regularly and kept updated in light of emerging risks and changing circumstances.

5.10. Material changes to the risk management strategy must be approved by the board of directors, properly justified and documented. The documentation must be available for review by internal audit, external audit, and the Prudential Authority, as needed.

6. Risk Management Policies[1]

6.1. An insurer must, at a minimum, have board-approved policies that address the following material risks and risk areas, where relevant:

a) asset-liability management;
b) capital management;
c) concentration;
d) credit;
e) fitness and propriety;
f) information technology;
g) insurance fraud;
h) investment;
i) liquidity management;
j) operational;
k) outsourcing;
l) reinsurance and other forms of risk transfer;
m) remuneration; and
n) underwriting.

6.2. An insurer may combine one or more of the policies for addressing risks specified in section 6.1 above, provided the insurer is of the view that the specified risks do not

[1] The policies listed in this section are a sub-set of the enterprise-wide policies required by this Standard. The policies in this section relate primarily to the prudent management of insurers. The section does not address policies related to conduct of business (such as sales and distribution practices), as these are dealt with by the Financial Services Conduct Authority. Nor does the section address policies that relate to non-financial areas such as human resources and workplace health and safety.

justify a separate policy given the nature, scale and complexity of the insurer's business and risks.

6.3. Attachment 1 (Policies for Managing Financial Risks) provides details on the required contents of the risk management policies specified in section 6.1 above.

6.4. An insurer's risk management policies must be reviewed regularly and kept updated in light of emerging risks.

6.5. Material changes to the risk management policies must be approved by the board of directors, properly justified and documented. The documentation must be available for review by internal audit, external audit, and the Prudential Authority as needed.

7. Risk Management Procedures and Tools

7.1. An insurer must maintain a suite of risk management procedures and tools that enables it to identify, assess, monitor, report on, and mitigate the material risks to which it is exposed. While the majority of material risks facing an insurer will typically be financial in nature, non-financial risks such as cyber risk must not be ignored. The suite must provide the board of directors with an enterprise-wide view of its material risks.

7.2. An insurer's suite of risk management procedures and tools must, at a minimum, include:

a) a process for identifying and assessing new and emerging risks;
b) procedures and tools for quantifying and managing specified individual material risks;
c) the application of scenario analysis and stress testing programs that are commensurate with the size, business mix and complexity of the insurer's business;
d) a forward-looking approach to assessing enterprise-wide financial risk through an Own Risk and Solvency Assessment process (ORSA) (see GOI 3.1 (Own Risk and Solvency Assessment (ORSA) for Insurers));
e) a management information system that provides reliable and informative reports on the measurement, assessment and management of all material risks; and
f) a review process to ensure the risk management system remains effective in identifying, quantifying, assessing and managing material risks to which the insurer is exposed.

7.3. An insurer's risk management procedures and tools must be reviewed regularly and kept updated in light of emerging risks and changes in the business risk profile.

7.4. Material changes to the risk management procedures and tools must be approved by the board of directors, properly justified and documented. The documentation must be available for review by internal audit, external audit, and the Prudential Authority as needed.

8. Internal Controls

8.1. An insurer's risk management system must be supported by an effective system of internal controls capable of providing the board of directors and senior management with reasonable assurance from a control perspective that the business is being operated consistently with:

a) the strategy and business objectives determined by the board of directors;

b) the key business, risk management, information technology and financial policies and procedures determined by the board of directors; and
c) the legislation that applies to the insurer.

8.2. An insurer's system of internal controls must be appropriate to the nature, scale and complexity of the insurer's business and risks.

8.3. At a minimum, an insurer's internal control system must provide for the following:

a) appropriate segregation of duties, and controls to ensure that segregation is observed;
b) appropriate controls for all key business processes and policies, including for major business decisions;
c) end-to-end control processes for complex business activities;
d) controls to provide reasonable assurance over the fairness, accuracy, reliability and completeness of the insurer's financial and non-financial information;
e) board-approved delegations of authority, (these should also be reviewed regularly by the board of directors);
f) controls at the appropriate levels, including at the procedure or transactional levels, and at the legal entity or business unit levels;
g) regular monitoring of all controls to ensure they remain effective;
h) an inventory of all key policies and procedures, and the controls in respect of each policy and procedure; and
i) training in respect of relevant components of the system of internal controls, particularly for employees in positions of trust or responsibility, or who carry out activities that involve significant risk.

9. Risk Governance - General Requirements for Control Functions

9.1. To provide appropriate governance over the risk management system and system of internal controls, an insurer must establish and adequately resource the control functions referred to in section 4.5 above. Control functions are a critical part of an insurer's checks and balances and must provide an independent perspective on risks and breaches of legal or regulatory requirements.

9.2. An insurer may, where appropriate in light of the nature, scale and complexity of the business, risks, and legal and regulatory obligations of an insurer, outsource a control function or a head of a control function (see GOI 5 (Outsourcing by Insurers)).

9.3. The board of directors must approve the roles and responsibilities, and any changes to the roles or responsibilities, of each control function, and must ensure that each function has the resources, authority and independence needed to meet its responsibilities.

9.4. The authority and responsibilities of each control function must be documented and subject to regular review by the board.

9.5. An insurer's control functions must be adequately staffed by appropriately qualified and competent persons who have sufficient authority to perform their roles effectively.

9.6. Control functions should operate without conflicts of interest; where a conflict arises, it must be brought to the attention of the board of directors for resolution.

9.7. Control functions must have the right to conduct investigations of possible breaches and to request assistance for such investigations from specialists within the insurer, or external specialists.

9.8. An insurer may, where appropriate in light of the nature, scale and complexity of the business, risks, and legal and regulatory obligations of an insurer, and subject to approval by the Prudential Authority, combine one or more control functions, with the exception that the internal audit function may not be combined with other control functions.

9.9. The board of directors, or relevant Committee, or an independent expert must periodically review and assess the performance of each control function.

9.10. Each control function must conduct regular self-assessments of their respective functions and implement or monitor the implementation of any needed improvements.

10. Risk Governance – Heads of Control Functions

10.1. Heads of control functions must be fit and proper (see GOI 4 (Fitness and Propriety of Key Persons ~~and Significant Owners~~ of Insurers)).

10.2. There must be adequate policies and procedures relating to the appointment, dismissal and succession of heads of control functions, and the board of directors must be actively involved in such processes.

10.3. The appointment, performance assessment, remuneration, disciplining and dismissal of the head of each control function (other than the head of the internal audit function) must be done with the approval of, or after consultation with, the board of directors or relevant board committee.

10.4. The appointment, performance assessment, remuneration, disciplining and dismissal of the head of the internal audit function must be done by the board of directors, its chairperson or the audit committee.

10.5. The remuneration of heads of control functions must not be predominantly linked to the financial performance of the insurer and must not be inconsistent with the long-term strategy and the financial soundness of the insurer. In addition, or where this function is outsourced the remuneration should be commensurate with the services provided.

10.6. Heads of control functions must have appropriate segregation of duties from operational business line responsibilities. The board of directors must ensure that the segregation is observed.

10.7. The heads of control functions must have:

a) sufficient seniority and authority to be effective;
b) reporting lines that support their independence;
c) unrestricted access to relevant information;
d) direct access to the board of directors or relevant Committee, without the presence of senior management if so requested, for the purpose of raising concerns about the effectiveness of the risk management system or system of internal controls; and
e) the freedom to report to the board of directors or relevant Committee without fear of retaliation from senior management.

10.8. An insurer may, where appropriate, in light of the nature, scale and complexity of the insurer's business and risks, and with the prior approval of the Prudential Authority, appoint a person as the head of more than one control function (other than the head of the internal audit function). Despite the aforementioned, the Prudential Authority may direct the insurer to appoint another or a dedicated person as the head of that control function, if the Prudential Authority is of the opinion that the person is not a suitable head for more than one control function.

10.9. Heads of control functions must report regularly to the board of directors or relevant Committee.

10.10. The head of a control function must without delay report in writing to the board of directors or relevant Committee any reasonable suspicion that any financial sector law relevant to its area that applies to the insurer has or is being contravened. Where the suspected contravention is of the Act or the Financial Sector Regulation Act, 2017, the head must also report immediately to the Prudential Authority if, in the opinion of the head, satisfactory steps to rectify the matter have not been taken within 30 days from the date of the board meeting at which the report is considered.

11. Risk Management Function

11.1. An insurer must have an effective risk management function, capable of assisting the board of directors and senior management to develop and maintain a risk management system to identify, assess, monitor, and mitigate the insurer's material risks, and promote a sound risk culture.

11.2. An insurer's risk management function is responsible for providing reasonable assurance that adequate mechanisms and procedures are established, implemented and maintained to:

a) identify the individual and aggregated risks (current and emerging) the insurer faces;
b) assess, monitor and help manage identified risks effectively;
c) gain and maintain an aggregated view of the risk profile of the insurer; and
d) establish a forward-looking assessment of the risk profile and financial position of the insurer, including the conducting of regular stress testing and scenario analyses as defined in GOI 3.1 (Own Risk and Solvency Assessment (ORSA) for Insurers), against the risk appetite and risk limits of the insurer.

11.3. An insurer's risk management function must assess the appropriateness of the insurer's policies, processes, and controls in respect of risk management and the effective monitoring thereof by the insurer.

11.4. The risk management function must:

a) regularly provide written reports to senior management, other key persons in control functions and the board of directors on the insurer's risk profile and details on the risk exposures facing the insurer and related mitigation actions as appropriate;
b) document and report material changes affecting the insurer's risk management system to the board of directors to help ensure that the system is maintained and improved; and
c) have access to and report to the board of directors or a committee of the board identified by the board of directors on the strategy of the risk management function and information on its resources, including an analysis on the appropriateness of those resources.

12. The Compliance Function

12.1. An insurer must have an effective compliance function capable of assisting the board of directors in overseeing and monitoring that the insurer meets its legal and regulatory obligations, and promotes and sustains a sound compliance culture.

12.2. An insurer's compliance function must implement a risk-based compliance monitoring plan to:

a) monitor compliance with the insurer's system of compliance related internal controls, as well as legal and regulatory obligations; and
b) identify, assess and report on key legal and regulatory risks.

12.3. An insurer's compliance function must assess the appropriateness of policies, processes, and controls in respect of key areas of legal, regulatory, and ethical obligations and the effective monitoring thereof by the insurer.

12.4. The compliance function must monitor compliance shortcomings and instances of non-compliance and, where required under section 10.10 above, report to the Prudential Authority or other relevant regulatory authorities.

12.5. An insurer's compliance function must ensure that regular training is conducted on compliance obligations, particularly for employees in positions of trust or responsibility, or who are involved in activities that have significant legal or regulatory risk.

12.6. Unless this role is assigned to another suitable function, an insurer's compliance function is responsible for ensuring that staff who wish to report concerns about the insurer are able to do so with appropriate protections.

12.7. The compliance function must have access to and report to the board of directors or a committee of the board identified by the board of directors on:

a) the strategy of the compliance function;
b) the compliance monitoring plan, including specific annual or other short-term goals being pursued and the performance against such goals; and
c) information on its resources, including an analysis on the appropriateness of those resources.

13. The Internal Audit Function

13.1. An insurer must have an effective internal audit function capable of providing the board of directors with independent assurance in respect of the adequacy and effectiveness of the insurer's corporate governance framework, and systems for risk management and internal control.

13.2. An insurer's internal audit function must also provide independent assurance to the board of directors, through regular audit activities, on matters such as:

a) the means by which the insurer preserves its assets and those of policyholders, and seeks to prevent fraud, misappropriation or misapplication of such assets;
b) the reliability, integrity and completeness of the accounting, financial and risk reporting information, as well as the capacity and adaptability of the insurer's information technology architecture to provide information in a timely manner to the board of directors and senior management;
c) the design and operational effectiveness of the insurer's controls in respect of the above matters;

d) other matters as may be requested by the board of directors, senior management, the Prudential Authority or the auditor; and
e) other matters which the internal audit function determines should be reviewed to fulfil its responsibilities as set out in its charter.

13.3. The head of an insurer's internal audit function must report directly to the board of directors or the audit committee. In its reporting, the internal audit function should address at least the following:

a) the function's annual or other periodic risk-based audit plan, detailing the proposed areas of audit focus, and any significant modifications to the audit plan;
b) any factors that may adversely affect the internal audit function's independence, objectivity or effectiveness;
c) material findings from audits or reviews conducted; and
d) the extent of senior management's compliance with agreed corrective or risk-mitigating measures in response to identified control deficiencies, system weaknesses, or compliance violations.

14. The Actuarial Function

14.1. An insurer must have an effective actuarial function capable of assisting the board of directors regarding the matters addressed below.

14.2. An insurer's actuarial function is responsible for expressing an opinion to the board of directors on the reliability and adequacy of the calculations of the insurer's technical provisions, and minimum and solvency capital requirements, including on:

a) the appropriateness of the methodologies and underlying models used and assumptions made;
b) the sufficiency and quality of the data used in actuarial calculations;
c) best estimates and associated assumptions against experience when evaluating technical provisions;
d) the accuracy of the calculations;
e) the appropriateness of and impact of assumed future management actions and the effect of risk mitigation instruments; and
f) the appropriateness of approximations or judgments used in the calculations due to insufficient data of appropriate quality.

14.3. An insurer's actuarial function is responsible for expressing an opinion to the board of directors on –

a) the appropriateness of the following policies of the insurer:
   i. Asset-liability Management Policy;
   ii. Underwriting Policy; and
   iii. Reinsurance and Other Forms of Risk Transfer Policy; and
b) the adequacy of reinsurance and other forms of risk transfer arrangements.

14.4. An insurer's actuarial function is responsible for evaluating and providing advice to the board of directors, senior management and other control functions (where relevant) on:

a) where the insurer uses the standardised formula to assess its risks, why that regulatory capital model is an accurate reflection of the insurer's own risk profile, taking into account the board-approved risk appetite (and related risk limits), and business strategy.

b) the development and use of internal models for internal actuarial or financial projections, or for own solvency projections as in the ORSA;
c) the insurer's investment policy;
d) the financial soundness position of the insurer, including the impact of any proposed dividend declaration or payment;
e) the actuarial-related matters in the ORSA such as the economic capital requirements, the forward looking projections of the economic and regulatory financial soundness positions, the stress-, sensitivity- and scenario testing, and the assumed management actions;
f) the internal controls relevant to actuarial matters referred to under this section 14;
g) the awarding of a bonus or similar benefit to participating policyholders in accordance with the principles and practises of financial management of the insurer; and
h) the actuarial soundness of the terms and conditions of insurance contracts.

Attachment 1: Policies for Managing Financial Risks

Principles

1. As part of prudent business management an insurer must have board-approved policies that address the identification and management of the risks it faces.

2. This Attachment provides details on the minimum required content of the financial and non-financial risk management policies set out in section 6.1 of the Standard.

3. Unless otherwise approved by the Prudential Authority, insurers must adopt the following policies and must address at least the issues raised in this Attachment.

A. Asset-Liability Management Policy

An insurer's asset-liability management policy must:

1. Clearly specify the nature, role and extent of the insurer's asset-liability management activities and their relationship with product development, pricing functions and investment management.

2. Co-ordinate the management of risks associated with assets and liabilities and the complexity of those risks.

3. Recognise the interdependence between the insurer's assets and liabilities and take into account the correlation of risk between different asset classes and the correlations between different products and business lines.

4. Take into account any off-balance sheet exposures that the insurer may have and the contingency that risks transferred may revert to the insurer.

B. Capital Management Policy

An insurer's capital management policy must:

1. Provide for an internal capital planning process.

2. Set out the insurer's strategy for ensuring adequate capital is maintained over time, including specific, quantifiable internal capital targets (excluding intra-group guarantees (where relevant)). These targets should be set taking into account the results of the insurer's ORSA reviews, the insurer's board-approved risk profile and risk appetite, and regulatory capital requirements. The strategy should include plans for how target levels of capital are to be met and the means available for sourcing additional capital where required. The strategy should be consistent with the insurer's overall business and risk management strategy.

3. Provide for the identification and measurement of risks that may result in capital shortfalls.

4. Establish procedures for monitoring the insurer's compliance with its regulatory and internal capital requirements and targets, including triggers to alert management to potential breaches of the regulatory and target capital requirements.

5. Set out the actions to be taken where capital shortfalls occur or are likely to occur.

6. Provide for appropriate management and regular review of capital and the capital management process (including independent review).

C. Concentration Risk Policy

An insurer's concentration risk policy must:

1. Identify relevant sources of concentration risk, and strategies and actions to be implemented to ensure that risk concentrations remain within established limits.

2. Analyse possible risks of correlation between concentrated exposures.

D. Credit Risk Policy

An insurer's credit risk policy must:

1. Set out the insurer's approach to the identification, assessment, monitoring, management, and reporting of credit risk. The insurer's approach to managing credit risk should be consistent with the complexity, risk profile, and scope of operations of the insurer.

2. Identify the full range of credit exposures the insurer is likely to encounter in its normal course of business. These should include direct credit exposures, such as through credit facilities and investments in debt instruments, and indirect credit exposures, such as those that arise through trading in financial instruments in organised financial markets, as well as short-term exposures to debtors and business partners.

3. Identify the range of credit exposures the insurer is willing to take on, and the ways in which it will avoid taking on those that it is unwilling to retain.

4. Provide for quantification of credit risks, using a methodology that is consistent with the complexity, risk profile, and scope of operations of the insurer.

5. Identify risk mitigation strategies for managing credit exposures to ensure they are kept within the credit risk limits set by the board of directors. Where risk mitigation involves risk transfer to another party, the insurer should ensure that the credit risk of the transferee is appropriately factored into the insurer's assessment of residual credit risk.

E. Fitness and Propriety Policy

For requirements relating to an insurer's fitness and propriety policy see section 5 of GOI 4 (Fitness and Propriety of Key Persons ~~and Significant Owners~~ of Insurers).

F. Information Technology Policy

An insurer's information technology policy must:

1. Provide for the development and implementation of an information technology internal control framework that:

    a) sets out the insurer's strategies, policies, systems, processes and controls relating to information technology and data quality;
    b) addresses the appropriateness, effectiveness, efficiency, integrity, confidentiality and reliability of the information technology and data quality systems of the insurer;
    c) facilitates compliance with legislative reporting requirements and legislation relating to confidentiality, privacy, security and retention of data or information; and

d) provides for independent assurance on the effectiveness of the information technology and data quality internal controls, including data management systems.

2. Address at least the following two critical technology-related risk areas:

   a) Cyber security risk – the risk of major disruption from a cyber-attack increases exponentially with advances in technology. The information technology policy must address the way in which the insurer will monitor cyber risk, respond to cyber-attacks, and manage cyber risk. Insurers must have a cyber-attack response plan, with clear assignment of roles and responsibilities for responding to the attack and keeping stakeholders informed.[2]
   b) Data privacy risk – insurers handle large volumes of sensitive personal information that is subject to privacy legislation. The information technology policy must address the way in which the insurer will monitor and protect data privacy.

3. Provide for processes to ensure the promotion of an ethical information technology governance culture and awareness of that culture (see GOI GN 2.1 (Corporate Culture))

4. Provide for processes and procedures to ensure the effective management and governance of information technology assets.

5. Provide for the development, implementation and management of systems for the management of information and data (including data quality), including systems in respect of information security and information management.

G. Insurance Fraud Risk Policy

An insurer's insurance fraud risk policy must:

1. Outline appropriate strategies, procedures and controls to deter, prevent, detect, report and remedy insurance fraud.

2. Outline appropriate strategies for managing fraud risk and the risk to the insurer's financial soundness or sustainability caused by fraud.

3. Take into consideration how the effectiveness of fraud risk management may be enhanced by contributing to industry-wide initiatives to deter, prevent, detect, report, and remedy insurance fraud.

4. Provide for the prompt reporting of insurance fraud to relevant regulatory authorities.

H. Investment Policy

An insurer's investment policy must:

1. Specify the nature, role and extent of the insurer's investment activities and how the insurer will ensure compliance with the asset requirements prescribed under the Financial Soundness Standards.

2. Set out the insurer's strategy for investing, including specifying asset allocation strategies, how these will be managed, and how they relate to the asset-liability management policy.

[2] Cyber risk is a central concern in business continuity planning (see GOI 3.2 (Business Continuity Management (BCM))).

3. Establish explicit risk management procedures with regard to more complex and less transparent classes of assets, including investments in markets or instruments that are subject to low levels of governance or regulation.

4. Take into account any factor which may materially affect the sustainable long-term performance of assets, including factors of an environmental, social and governance character.

5. Adhere to the 'Prudent Person Principle' by establishing measures that will assist in ensuring that:

    a) the insurer invests only in assets and instruments whose risks the insurer can properly identify, assess, monitor, manage, control, and report on; and
    b) assets are invested in a manner appropriate to the nature and duration of the insurer's liabilities and the best interests of policyholders and beneficiaries.

6. Ensure that investments are made in a manner that ensures the security, quality, liquidity and profitability of the insurer's whole portfolio.

7. Ensure that investments in assets that do not trade on a regulated financial market are kept to prudent levels.

8. Ensure that investments are diversified in a manner that avoids excessive reliance on any particular asset, issuer or group of companies, or geographical area and excessive concentration of risk in the portfolio as a whole.

9. Ensure that conflicts of interest are avoided or managed so that investments are made in the best interests of policyholders and beneficiaries.

10. Notwithstanding the diversification requirement of sub-section 8 above, ensure that where assets are held in respect of long-term policies, where the investment risk is borne by the policyholders, the corresponding liabilities are:

    a) in the case of insurance obligations that are directly linked to the value of units, represented as closely as possible by those units; and
    b) in the case of insurance obligations that are linked directly to a share index or a reference value other than units, represented as closely as possible by the units deemed to represent the reference value or, in the case where units are not established, by assets of appropriate security and marketability which correspond as closely as possible with those on which the particular reference value is based.

11. Ensure that, in the case where investment performance is guaranteed, appropriate assets are held to support the guarantee.

I. Liquidity Management Policy

An insurer's liquidity management policy must:

1. Set out the insurer's approach to the identification, assessment, monitoring, management, and reporting of short-term and long-term liquidity risk, to ensure that the insurer is able to meet its obligations as they fall due. The insurer's approach to managing liquidity risk should be consistent with the complexity, risk profile, and scope of operations of the insurer. The approach must include triggers, action plans, and clear responsibilities for responding to liquidity stresses, should they arise.

2. Include modelling the impact on the insurer's liquidity of a range of adverse scenarios. These scenarios should include major trigger events such as

catastrophes, downgrades from rating agencies, counterparty defaults, and other adverse events.

3. Take specific account of the liquidity consequences of financial difficulties or default by its reinsurance counterparties, and the types of events that could lead to such difficulties.

4. Take specific account of the nature of the insurer's investments and the impact of adverse scenarios on the liquidity of these investments.

J. Operational Risk Policy

An insurer's operational risk policy must:

1. Set out the insurer's approach to the identification, assessment, monitoring, management and reporting of relevant operational risk exposures (including the risks associated with inadequate or failed internal processes, people or systems, or from external events).

2. To the extent quantitative data on incidents and impacts are available, the insurer should leverage those data to help quantify operational risks. Where possible, and legally permissible, the insurer should share such data with industry and leverage broader industry experience to help quantify operational risks.

K. Outsourcing Policy

1. For requirements relating to an insurer's outsourcing policy see section 5 of GOI 5 (Outsourcing by Insurers).

L. Reinsurance and Other Forms of Risk Transfer Policy

1. For requirements relating to an insurer's reinsurance and other forms of risk transfer policy see section 5 of GOI 3.3 (Reinsurance and Other Forms of Risk Transfer by Insurers).

M. Remuneration Policy

An insurer's remuneration policy must:

1. Not induce excessive or inappropriate risk taking and be consistent with the long-term interests of the insurer and the interests of its policyholders.

2. At a minimum, address the remuneration of key persons and other persons whose actions may have a material impact on the risk exposure of the insurer (including persons to whom /functions are outsourced).

3. Be consistent with the insurer's business and risk management strategy (including risk management practices), and target corporate culture (see GOI GN 2.1 (Corporate Culture)).

4. Apply to the insurer as a whole in a proportionate and risk-based way and contain specific arrangements that take into account the respective roles of persons referred to in sub-section 2.

5. Provide for a clear, transparent, and effective governance structure around remuneration, and oversight of the policy.

6. When remuneration includes both fixed and variable components, provide that:

a) the fixed portion represents a sufficiently high portion of the total remuneration to avoid over dependence on the variable components;
b) the variable component is based on a combination of the assessment of the individual and the collective performance, such as the performance of the business area and the overall results of the insurer; and
c) the payment of the major part of a significant bonus, irrespective of the form in which it is to be paid, contains a flexible, deferred component that considers the nature and time horizon of the insurer.

7. Ensure that, in defining an individual's performance, that both financial (where relevant) and non-financial performance are considered.

N. Underwriting Policy

An insurer's underwriting policy must:

1. Identify the nature of the insurer's insurance business, including, but not limited to:

    a) the classes of insurance to be underwritten; and
    b) the types of risks that may be underwritten and those that are to be excluded.

2. Describe the formal risk assessment process for underwriting, including, but not limited to:

    a) the criteria used for risk assessment;
    b) the method(s) for monitoring emerging experience; and
    c) the method(s) by which emerging experience is taken into consideration in the underwriting process.

3. Establish decision-making processes and controls where non-mandated intermediaries or underwriting managers perform binder functions on behalf of the insurer in accordance with Part 6 of the Regulations made under the Long-term Insurance Act, 1998 or the Short-term Insurance Act, 1998.

4. Set out the actions to be taken by the insurer to assess and manage the risk of loss, or of adverse change in the values of insurance and reinsurance liabilities, resulting from inadequate pricing and provisioning assumptions.

5. Establish the insurer's approach to assumption setting, including the level of conservatism need to align with the insurer's risk appetite.

6. Set out the relevant data (quantity and quality) to be considered in the underwriting and reserving processes.

7. Provide for the regular review of the adequacy of claims management procedures, including the extent to which they cover the overall cycle of claims.