BOARD NOTICE

NOTICE 114 OF 2014

FINANCIAL SERVICES BOARD

REGISTRAR OF LONG-TERM INSURANCE AND SHORT-TERM INSURANCE

LONG-TERM INSURANCE ACT, 1998 (ACT NO. 52 OF 1998) AND SHORT-TERM INSURANCE ACT, 1998 (ACT 53 OF 1998)

PROPOSED GOVERNANCE AND RISK MANAGEMENT FRAMEWORK FOR INSURERS

I, Dube Phineas Tshidi, Registrar of Long-term Insurance and Registrar of Short-term Insurance, hereby, under the Long-term Insurance Act, 1998 (Act No. 52 of 1998) and Short-term Insurance Act, 1998 (Act No. 53 of 1998) ("the Acts"), publish for public comment, as set out in Schedule A hereto, the proposed governance and risk management framework to be prescribed pursuant to sections 12(1)(bD) of the Acts.

Section 12 was amended through the Financial Services Laws General Amendment Act, 2013 (Act No. 45 of 2013) to provide that the Registrar may prescribe such a framework, and came into effect on 28 February 2014.

The proposals set out in the Schedule –

- give effect to the governance, risk management and internal control measures mooted in the Insurance Laws Amendment Bill, 2013, which was withdrawn by the Minister of Finance due to the Parliamentary schedule;
- take into account the public comments submitted to the National Treasury on the draft Insurance Laws Amendment Bill during 2012, and reflect key areas of agreement reached on changes to the Bill at meetings and workshops convened with key affected stakeholders to discuss these public comments (a response to the public comments received on the Bill was issued by the National Treasury on 29 April 2014 and is available on the websites of the National Treasury and the Financial Services Board); and
- give effect to international standards as set out in the Insurance Core Principles of the International Association of Insurance Supervisors (October 2013).

It is envisaged that the final requirements and framework will be published by the end November 2014 for implementation by 1 April 2015.

Comments on the proposed amendment may be submitted in writing on or before 7 November 2014 to the Registrar at FSB.INSGRMF@fsb.co.za.

DP TSHIDI
Registrar of Long-term Insurance and Registrar of Short-term Insurance

SCHEDULE A

Arrangement of sections

PART 1: INTERPRETATION

Definitions

1. In this Schedule any word or expression to which a meaning has been assigned in the Long-term Insurance Act, 1998 (Act No. 52 of 1998) or Short-term Insurance Act, 1998 (Act No. 53 of 1998), as the case may be, has the same meaning, and, unless the context indicates otherwise –

"control function" means –

(a) the risk management function;

(b) the compliance function;

(c) the actuarial function;

(d) internal audit function; or

(e) all of these functions;

"head of a control function" means the employee of the insurer that is in charge of a control function;

"insurer" means a long-term insurer or a short-term insurer, as the case may be;

"regulatory authority[1]" has the meaning set out in section 1 of the Financial Services Board Act;

"significant owner" means a person that acquired or holds shares or any other financial interest in an insurer within the meaning of section 26 of the Long-term Insurance Act, 1998 or section 25 of the Short-term Act, 1998, as the case may be; and

"outsourced" has the meaning set out in Directive 159.A.i: *Compliance with sections 9(3)(b)(i) read with sections 12(1)(c) of the Long-term Insurance Act and Short-term Insurance Act, respectively: Outsourcing*, 12 April 2012, and "outsource" and "outsourcing" has the a corresponding meaning[2];

"the Act" means the Long-term Insurance Act, 1998 or the Short-term Insurance Act, 1998, as the case may be.

---

[1] "regulatory authority" means -
(a) any organ of state as defined in section 239 of the Constitution of the Republic of South Africa, 1996, responsible for the supervision or enforcement of legislation, or a similar body designated in the laws of a country other than the Republic to supervise or enforce legislation of that country; or
(b) a market infrastructure that is responsible for the supervision of persons authorised by such infrastructure under the Financial Markets Act, 2012 (Act No. 19 of 2012); or
(c) an Ombud established under Financial Services Board legislation or a recognised Scheme under the Financial Services Ombud Schemes Act, 2004 (Act No. 37 of 2004);

[2] Outsourcing and insourcing is not provided for in this Notice. In respect of outsourcing, Directive 159.A.i continues to apply.

PART 2: GOVERNANCE AND RISK MANAGEMENT FRAMEWORK – GENERAL

Governance framework

2. (1) An insurer must adopt, implement and document an effective governance framework that provides for the prudent management and oversight of its insurance business and adequately protects the interests of its policyholders.

(2) The governance framework must be proportionate to the nature, scale and complexity of the insurer's business and risks and must address and provide for, at least, the matters provided for in Parts 3 to 5.

(3) The Registrar at any time may –

(a) require the board of directors or senior management, or both, of the insurer to demonstrate that the governance framework requirements provided for in this Board Notice are being complied with; or

(b) direct an insurer to secure an independent review of the governance framework by a person nominated by the Registrar at the cost of the insurer; and

(c) direct the insurer, its board of directors or senior management, or both, to strengthen and effect improvements to its governance framework or a part thereof.

PART 3: COMPOSITION, GOVERNANCE AND STRUCTURE OF THE BOARD OF DIRECTORS

Board of directors

Composition and governance of board of directors

3. (1) For purposes of this section[3], -

(a) a non-executive director means an individual who is not involved in the day-to-day management of the insurer or has not been so involved at any time during the previous financial year; and

(b) an independent director –

(i) means a non-executive director that –

[3] These requirements are based on the requirements for members of audit committees as set out in the Companies Act.

(aa) is not and has not in the past three financial years been an employee of the insurer or any of its related or inter-related persons (as defined in section 1 of the Companies Act);

(bb) is not a member of the immediate family of an individual mentioned in subparagraph (aa); or

(cc) is not a material supplier or customer of the insurer, such that a reasonable and informed third party would conclude in the circumstances that the integrity, impartiality or objectivity of that director is compromised by that relationship; and

(ii) includes a director of the direct or indirect holding company of the insurer that meets the requirements set out in paragraph (i) in respect of that holding company.

(2)(a) The board of directors of an insurer must at all times consist of -

(i) a sufficient number of non-executive directors and independent directors to promote objectivity in decision-making by the board of directors; and

(ii) an appropriate number and mix of individuals to ensure that there is an overall adequate spread and level of knowledge, skills and expertise at board level commensurate with the nature, scale and complexity of the business and risks of the insurer;

(b) If paragraph (a) is not complied with, the board of directors must notify the Registrar of the composition of the board of directors and motivate to the Registrar why the composition of the board of directors does not undermine the effectiveness of the insurer's governance framework.

(3)(a) The chairperson of the board of directors of an insurer must be an independent director.

(b) If subsection (a) is not complied with, the board of directors must –

(i) appoint a lead independent director; and

(ii) notify the Registrar of the non-compliance with paragraph (a) and motivate to the Registrar why the non-compliance does not undermine the effectiveness of the insurer's governance framework.

(4) Despite subsections (2) and (3), the Registrar to ensure the prudent management of the insurer's insurance business and protection of the interests of policyholders may direct the board of directors to -

(a) change the composition of the board of directors;

(b) appoint another person as independent chairperson; or

(c) appoint another person as lead independent director.

(5) The board of directors of an insurer must –

(a) have appropriate internal governance practices and procedures to support its work in a manner that promotes efficient, objective and independent judgment and decision-making;

(b) have adequate powers and resources to discharge its duties fully and effectively; and

(c) adopt and implement a procedure to review, at least annually, its performance collectively, and that of each director individually.

Roles and responsibilities of board of directors

4. (1) The board of directors is accountable for the effective governance and risk management of an insurer.

(2) The board of directors of an insurer must -

(a) determine and oversee the implementation of the insurer's business objectives and strategies for achieving those objectives, which objectives and strategies must be regularly reviewed to be consistent with the long-term interests and viability of the insurer and the interests of its policyholders;

(b) ensure that the roles and responsibilities allocated to the board of directors, managing executives and heads of control functions are clearly defined so as to promote an appropriate separation of oversight function from management responsibilities;

(c) ensure that there are adequate policies and procedures relating to the appointment, dismissal and succession of managing executives and heads of control functions;

(d) provide oversight in respect of the design and implementation of sound risk management and internal control systems and functions;

(e) adopt and oversee the effective implementation of all material policies and procedures of the insurer, including, but not limited to, the overall risk management policy and component policies referred to in section 11;

(f) monitor compliance with its fit and proper policy to facilitate the sound and prudent management of the business of the insurer;

(g) ensure reliable and transparent financial reporting for public and supervisory purposes;

(h) have systems and controls to ensure the promotion of appropriate, timely and effective communications with the Registrar on the governance framework of the insurer, which will allow the latter to make informed judgments about the effectiveness of the board of directors and managing executives in governing the

insurer;

(i) have appropriate policies and procedures to oversee that managing executives -

(i) carry out the day-to-day operations of the insurer effectively and in accordance with the insurer's strategies, policies and procedures;

(ii) promote a culture of sound risk management, compliance and policyholder protection;

(iii) provide the board of directors with adequate and timely information to enable it to carry out its duties and functions, including the monitoring and review of the performance and risk exposures of the insurer, and the performance of managing executives; and

(iv) provide the Registrar and relevant stakeholders with the information required to satisfy the legal and other obligations applicable to the insurer; and

(j) regularly monitor and evaluate the adequacy and effectiveness of the insurer's governance framework and notify the Registrar of any shortcomings and the reasons therefore.

(3) (a) The board of directors may delegate some of the activities or tasks associated with its roles and responsibilities to a board committee, a managing executive or any other person within the insurer.

(b) The board of directors of an insurer must develop an appropriate system of delegation, which delegation must -

(i) be appropriately and clearly mandated;

(ii) provide adequate checks and balances;

(iii) provide for the monitoring and reporting on delegations;

(iv) not allow for the undue concentration of powers; and

(v) provide for the withdrawal of a delegation.

(c) Anything done or omitted to be done under a delegation—

(i) does not in any way abrogate the accountability of the board of directors; and

(ii) is deemed to have been done or omitted by the board of directors.

Duties of each director

5. Each director of an insurer, in addition to the requirements of the Companies Act, must -

(a) at all times comply with the fit and proper policy of the insurer;

(b) act in the best interests of the insurer and policyholders, putting the interests of the insurer and policyholders ahead of his or her own interests; and

(c) exercise independent judgment and objectivity in decision-making, taking into account the interests of the insurer and policyholders.

Committees of the board

Structure of board of directors

6. (1) The board of directors of an insurer must assess whether, and to what extent, the establishment of committees of the board is necessary and appropriate.

(2) Committees of the board must -

(a) be structured to ensure that they have the necessary authority, independence, resources and expertise;

(b) have access to all relevant employees and information to perform their functions; and

(c) have a clearly defined and documented mandate and functions.

Risk and remuneration committees

7. (1) Despite section 6, an insurer must establish a risk committee and a remuneration committee.

(2) A risk committee must comprise of at least three members that include executive and non-executive directors, and members of senior management, and perform, at least, the functions as set out in section 8.

(3) A remuneration committee must comprise of at least three members of the board of directors of which the majority must be non-executive directors and perform, at least, the functions as set out in section 9.

(4) The chairperson of the risk or remuneration committee must be an independent director of the board of directors.

(5) If a risk committee, a remuneration committee or both these committees are not established the board of directors must –

(a) notify and motivate the non-compliance with subsection (1) to the Registrar; and

(b) ensure that the functions of these committees are performed by the audit committee (despite the composition requirements set out in subsections (2) and (3))[4] or another committee approved by the Registrar.

(6) Despite subsection (5), the Registrar to ensure the prudent management of the insurance business and protection of the interests of policyholders may instruct the board of directors to –

(a) establish one or both of these committees; or

[4] Note that an audit committee as per the Companies Act must consist of independent directors only.

(b) change the composition of either or both of the committees.

Risk Committee

8. A risk committee must perform the following functions:

(a) assist the board of directors in its evaluation of the adequacy and efficiency of the risk management system;

(b) assist the board of directors in the identification of the build-up and concentration of the various risks to which the insurer is exposed;

(c) assist the board of directors in identifying and regularly monitoring all material risks and key performance indicators to ensure that its decision-making capability and accuracy of its reporting is maintained at a high level;

(d) facilitate and promote communication, through reporting structures, regarding the matters referred to in paragraph (a) or any other related matter, between the board of directors and managing executives;

(e) ensure the establishment of an independent risk management function;

(f) introduce such measures as may serve to enhance the adequacy and efficiency of the risk management system; and

(g) co-ordinate the monitoring of risk management on an enterprise-wide basis.

Remuneration Committee

9. A remuneration committee must perform the following functions:

(a) develop an appropriate remuneration policy referred to in section 13; and

(b) implement, monitor and regularly review the suitability of an insurer's remuneration policy.

PART 4: RISK MANAGEMENT SYSTEM

Risk management system

10. (1) An insurer must establish and maintain an effective risk management system, comprising the totality of strategies, policies and procedures for identifying, assessing, monitoring, managing, and reporting of all material risks to which the insurer may be exposed.

(2) The risk management system must –

(a) adequately support the board of directors in meeting its responsibilities with respect

to the furtherance of the safe and sound operation of the insurer and the protection of policyholders, taking into account the nature, scale and complexity of the of the insurer's business and risks;

(b) address risks on an enterprise-wide basis; and

(c) be embedded within the organisation of the insurer.

(3) The risk management system must, at least, include -

(a) a clearly defined and well documented risk management strategy which takes into account the insurer's overall business strategy (as approved by the board of directors) and its business activities (including any business activities which have been outsourced);

(b) documented procedures which clearly define the decision-making processes within the framework of the risk management system;

(c) an adequate written overall risk management policy and component policies consistent with the risk management strategy referred to in paragraph (a) and the requirements of sections 11 to 23;

(d) appropriate processes, procedures and tools (including, where appropriate, models) for identifying, assessing, monitoring, managing, and reporting (including communication and escalation mechanisms) on each material risk;

(e) reports (regular and *ad hoc*) to inform the managing executives and the board of directors on the risk profile of the insurer, including each material risk faced by the insurer and on the effectiveness of the risk management system itself; and

(f) processes for ensuring adequate contingency planning, business continuity and crisis management.

(4) (a) The risk management system must be reviewed regularly by the internal audit function or an objective external reviewer of the insurer to ensure that the system is effective and that necessary modifications are identified and made in a timely manner.

(b) The risk management system and any modifications must be documented and approved by the board of directors.

Overall risk management policy

11. (1) An insurer must develop and regularly review an adequate written overall risk management policy that includes –

(a) a definition and categorisation of the material risks (including external and internal business specific and enterprise-wide risks, both current and emerging) to which the insurer is exposed, taking into account the nature, scale and complexity of the

insurer and its business;

(b) the approach of the insurer to assessing the materiality of the risks referred to in paragraph (a);

(c) the approach relating to the identification, assessment, monitoring, management and reporting of each, including assignment of specific risk management obligations across the insurer; and

(d) at least, the following distinct component policies:

(i) a fit and proper policy that provides for the matters provided for under section 12;

(ii) a remuneration policy that provides for the matters provided for under section 13;

(iii) an asset-liability management policy that provides for the matters provided for under section 14;

(iv) an investment policy that provides for the matters provided for under section 15;

(v) an underwriting risk management policy that provides for the matters provided for under section 16;

(vi) a reinsurance and other forms of risk transfer policy that provides for the matters provided for under section 17;

(vii) a liquidity risk management policy that that provides for the matters provided for under section 18;

(viii) a concentration risk management policy that that provides for the matters provided for under section 19;

(ix) an operational risk management policy that that provides for the matters provided for under section 20;

(x) an information technology governance policy that provides for the matters provided for under section 21;

(xi) an insurance fraud risk management sub-policy that provides for the matters provided for under section 22; and

(xii) in the case of a long-term insurer, an anti-money laundering and combatting the financing of terrorism policy that provides for the matters provided for under section 23.

(2) Despite subsection (1)(d), an insurer may combine the component policies referred to in subsection (1)(d) or provide for the component policy in the overall risk management policy if the insurer is of the view that the specific risks referred to in

that paragraph do not justify a distinct policy given the nature, scale and complexity of the insurer's business and risks.

Fit and proper policy

12. An insurer's fit and proper policy must, at least, –

(a) provide for the prudent management of the risks that a director, managing executive, public officer, auditor, statutory actuary (or his or her alternate), head of a control function or significant owner (collectively referred to as "responsible person") who are not fit and proper pose to its insurance business, financial soundness and fair treatment of customers;

(b) clearly define and document the fit and proper criteria required for each responsible person having regard to–

(i) any prescribed fit and proper requirements; and

(ii) the need to set high internal standards of ethics and integrity that promote sound corporate governance and appropriate and pertinent expertise, educational qualifications or experience, skills and knowledge in respect of the duties that such a person must perform;

(c) include the processes (including the decision-making processes) to be undertaken in assessing whether a responsible person is fit and proper;

(d) specify the actions to be taken where the insurer assesses a responsible person as not being fit and proper, which must include notifying the Registrar of such an assessment and the actions taken;

(e) require periodic (at least annual) fit and proper assessments for each responsible person;

(f) require that sufficient documentation for each fit and proper assessment is retained to demonstrate the fitness and propriety of responsible persons and their immediate predecessors;

(g) include adequate provisions to allow whistleblowing if a person believes that a responsible person does not meet the insurer's fit and proper criteria and for the protection of such a person;

(h) provide that responsible persons consent to being subject to the fit and proper policy; and

(i) provide that the insurer consents to any former responsible person disclosing information to the Registrar, including their reasons for resignation, early retirement or removal.

Remuneration policy

13. (1) For purposes of this section, the term "remuneration" has the meaning as defined in section 30(6) of the Companies Act.

(2) An insurer's remuneration policy must –

(a) not induce excessive or inappropriate risk taking and be consistent with the long-term interests of the insurer and the interests of its policyholders;

(b) at a minimum, address the remuneration of directors, managing executives, heads of control functions and other persons whose actions may have a material impact on the risk exposure of the insurer (including persons to whom functions are outsourced);

(c) be consistent with the insurer's business and risk strategy (including the insurer's risk management practices), and performance;

(d) 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 paragraph (b);

(e) provide for a clear, transparent and effective governance structure around remuneration, and the oversight of the policy;

(f) when remuneration includes both fixed and variable components, provide that –

(i) the fixed portion represents a sufficiently high proportion of the total remuneration to avoid over dependence on the variable components and allow the insurer to operate a fully flexible bonus policy;

(ii) 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

(iii) 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's business; and

(g) ensure that in defining an individual's performance, that financial and non-financial performance are considered.

Asset-liability management policy

14. An insurer's asset-liability management policy must –

(a) 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;

(b) co-ordinate the management of risks associated with assets and liabilities and the complexity of those risks;

(c) 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; and

(d) take into account any off-balance sheet exposures that the insurer may have and the contingency that risks transferred may revert to the insurer.

Investment policy

15. (1) An insurer's investment policy must –

(a) provide for the investment of all the insurer's assets in accordance with the Act;

(b) specify the nature, role and extent of the insurer's investment activities and how the insurer complies with the value of and limitations on assets requirements as prescribed under the Act;

(c) set out the insurer's strategy for optimising investment returns and specify asset allocation strategies and authorities for investment activities and how these are related to the asset-liability management policy;

(d) establish explicit risk management procedures with regard to more complex and less transparent classes of asset and investment in markets or instruments that are subject to less governance or regulation;

(e) take into account the *Code for Responsible Investing by Institutional Investors in South Africa, 2011* (as may be amended from time to time) as issued by the Committee on Responsible Investing by Institutional Investors in South Africa; and

(f) adhere to the 'Prudent Person Principle' by establishing measures that will assist in ensuring that –

(i) the insurer only invests in assets and instruments whose risks the insurer can properly identify, assess, monitor, manage, control, and report on; and

(ii) 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.

(2) An insurer's investment policy must provide in respect of -

(a) the investment of all assets, specifically those assets covering the financial soundness requirements, for investment in a manner that ensures the security, quality, liquidity and profitability of its whole portfolio of assets and the availability of assets;

(b) a conflict of interest, that investments are made in the best interest of policyholders and beneficiaries;

(c) assets held in respect of long-term policies where the investment risk is borne by the policyholders, that the liabilities must –

(i) in the case of policy benefits that are directly linked to the value of units, be represented as closely as possible by those units;

(ii) in the case of policy benefits that are directly linked to a share index or a reference value other than units, be represented as closely as possible 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;

(d) benefits referred to under paragraph (c)(i) or (ii) that include a guarantee of investment performance or another guaranteed benefit, for assets held to cover the corresponding additional liabilities to adhere to subsection (1)(f)(ii); and

(e) assets other than those referred to under paragraph (c), for -

(i) investments in derivative instruments only if the instruments contribute to a reduction of risks or facilitate efficient portfolio management;

(ii) investments in assets which are not admitted to trading on a regulated financial market only if such investments are kept to stated prudent levels;

(iii) the proper diversification of assets in a manner that avoids excessive reliance on any particular asset, issuer or group of companies, or geographical area and excessive accumulation of risk in the portfolio as a whole.

Underwriting risk management policy

16. The underwriting risk management policy must –

(a) identify the nature of the insurer's insurance business, including, but not limited to –

(i) the classes of insurance to be underwritten; and

(ii) the types of risks that may be underwritten and those that are to be excluded;

(b) describe the formal risk assessment process in underwriting, including, but not limited to-

(i) the criteria used for risk assessment;

(ii) the method(s) for monitoring emerging experience; and

(iii) the method(s) by which the emerging experience is taken into consideration in the underwriting process;

(c) provide for 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 Act;

(d) 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;

(e) set out the relevant data (quantity and quality) to be considered in the underwriting and reserving processes; and

(f) provide for the regular review of the adequacy of claims management procedures, including the extent to which they cover the overall cycle of claims.

Reinsurance and other forms of risk transfer policy

17. An insurer's reinsurance and other forms of risk transfer policy must –

(a) outline appropriate strategies and procedures for the selection of suitable reinsurance programs and other risk transfer techniques, proportionate to the nature, scale and complexity of the insurer's risks, and to the capabilities of the insurer to manage and control the risk transfer technique used;

(b) ensure transparent reinsurance arrangements and associated risks that enable the Registrar to understand the economic impact of reinsurance and other forms of risk transfer arrangements in place;

(c) provide for processes and procedures for ensuring that the strategies referred to in paragraph (a) are implemented and complied with, and that the insurer has in place appropriate systems and controls over its risk transfer transactions;

(d) identify the level of risk transfer appropriate to the insurer's approach to risk;

(e) identify the types of reinsurance arrangements most appropriate to effectively manage the insurer's risk profile;

(f) identify principles for the selection of reinsurance counterparties;

(g) provide for procedures for assessing the creditworthiness and diversification of reinsurance counterparties;

(h) provide for procedures for assessing the effectiveness of the risk transfer;

(i) set concentration limits for credit risk exposure to reinsurance counterparties and appropriate systems for monitoring these exposures; and

(j) provide for liquidity management to address any timing mismatch between claims' payments and reinsurance recoveries.

Liquidity risk management policy

18. The liquidity risk management policy must set out the approach to the identification, assessment, monitoring, management and reporting of short-term and long-term liquidity risk, including a plan to address changes in expected cash in-flows and out-flows, in order

to meet the insurer's obligations as they fall due.

Concentration risk management policy

19. The concentration risk management policy must set out the actions to be taken to –
    (a) identify relevant sources of concentration risk to ensure that risk concentrations remain within established limits; and
    (b) analyse possible risks of contagion between concentrated exposures.

Operational risk management policy

20. The operational risk management policy must set out the 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).

Information technology governance policy

21. The insurer's information technology governance policy must provide for -
    (a) the development and implementation of an information technology internal control framework that -
        (i) addresses planning, implementation, delivery, support, monitoring and reporting;
        (ii) addresses effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance; and
        (iii) provides for independent assurance on the effectiveness of the information technology internal controls, including data management systems;
    (b) processes for ensuring the promotion of an ethical information technology governance culture;
    (c) processes and procedures to ensure the effective management of information technology assets; and
    (d) the development and implementation of systems for the management of information and data, including systems in respect of information security and information privacy.

Insurance fraud risk management policy

22. The insurance fraud risk management policy must –

(a) outline appropriate strategies, procedures and controls to deter, prevent, detect, report and remedy insurance fraud, and to effectively manage fraud risk and possible risks to the insurer's financial soundness or business continuity caused by fraud;

(b) provide for regular internal fraud-sensitive audits;

(c) provide for participation in industry-wide initiatives to deter, prevent, detect, report and remedy insurance fraud; and

(d) provide for the prompt reporting of insurance fraud to relevant regulatory authorities and entities established by industry associations for the deterrence, prevention, detection and investigating of insurance fraud.

Anti-money laundering and combatting the financing of terrorism policy

23. The anti-money laundering and combatting the financing of terrorism policy must –

(a) outline appropriate strategies, procedures and controls to deter, prevent, detect, report and remedy money laundering and the financing of terrorism; and

(b) provide for the prompt reporting of money laundering and the financing of terrorism to relevant regulatory authorities in accordance with legislative requirements.

PART 5: INTERNAL CONTROL SYSTEM

Internal control system

24. (1) An insurer must establish, maintain and operate within an effective internal control system, comprising the totality of strategies, policies, procedures and controls to assist the board of directors and managing executives in the fulfillment of their respective responsibilities for oversight and management of the insurer, as the case may be.

(2) The internal control system must be appropriate to the nature, scale, and complexity of the insurer's business and risks and provide the board of directors and managing executives with reasonable assurance from a control perspective that the insurance business is operated consistently with –

(a) the strategy determined by the board of directors;

(b) the business objectives of the insurer;

(c) the key business, information technology and financial policies and processes, and related risk management policies and procedures, determined by the board of directors; and

(d) the legislation that applies to the insurer.

(3) The internal control system must, at least, provide for -

(a) appropriate controls to ensure the availability and reliability of financial and non-financial information;

(b) the development, implementation and regular review of a compliance plan that provides for the matters provided for in section 27;

(c) appropriate segregation of duties, and controls to ensure that such segregation is observed;

(d) regular monitoring of all controls to ensure that –

(i) the totality of controls forms a coherent system; and

(ii) the internal control system –

(aa) functions as intended;

(bb) fits within the overall governance framework; and

(cc) complements the risk identification, risk assessment, and risk management activities of the insurer;

(e) regular independent testing and assessments to determine the adequacy, completeness and effectiveness of the internal control system and its usefulness to the board of directors and managing executives for controlling the operations of the insurer;

(f) appropriate controls to provide reasonable assurance over the fairness, accuracy, and completeness of the insurer's financial statements, records and accounts;

(g) appropriate controls for other key business procedures and policies, including major business decisions and transactions, critical information technology functionalities, access to databases and information technology systems by employees, and important legal and regulatory obligations;

(h) up-to-date policies regarding who may sign on behalf of or commit the insurer, and for what amounts, with corresponding controls, such as the requirement of double or multiple signatures;

(i) controls at the appropriate levels so as to be effective, including at the procedure or transactional level, and at the legal entity or business area level;

(j) a centralised written inventory of key procedures and policies insurer-wide, and of the controls in place in respect of such procedures and policies; and

(k) training in respect of the internal control system, particularly for employees in positions of trust or responsibility, or carrying out high risk activities.

General requirements for control functions

25. (1) An insurer must establish and maintain the following control functions:

(a) a risk management function;

(b) a compliance function;

(c) an internal audit function; and

(d) in the case of a long-term insurer, an actuarial function.

(2) The Registrar may exempt a long-term insurer from the requirement to establish and maintain an actuarial function if the Registrar is of the opinion that it is appropriate given the nature, scale and complexity of the insurer's business and risks.

(3) Each control function referred to in subsection (1) must be structured to ensure that the function has the necessary authority, independence, resources, expertise and access to the board of directors and all relevant employees and information to exercise its authority and perform its responsibilities.

(4) The authority and responsibilities of each control function must be determined and documented under the governance framework of the insurer referred to under Part 2.

(5) (a) The risk management function, compliance function and actuarial function must be regularly reviewed by the insurer's internal audit function or an objective external reviewer.

(b) The internal audit function must be regularly reviewed by an objective external reviewer.

(c) The board of directors must regularly review the performance of each control function, taking into consideration the reviews referred to under paragraphs (a) and (b).

(6) The existence of any control function does not relieve the board of directors or managing executives from their respective governance and related responsibilities.

(7) 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.

(8) Each control function must –

(a) avoid conflicts of interest, and if any conflict cannot be avoided report that conflict to the executive managers and the board of directors; and

(b) comply with the requirements relating to the reporting structures, independence, resources, expertise, responsibilities and functions referred to in sections 26 to 29.

Risk management function

26. (1) The insurer's risk management function must establish, implement and maintain appropriate mechanisms and activities (including a strategy and operational plan) to:

(a) assist the board of directors and managing executives in carrying out their respective responsibilities, including by providing specialist analysis and performing

risk reviews;

(b) identify the risks the insurer faces;

(c) assess, aggregate, monitor and assist in managing and otherwise addressing identified risks effectively (including assessing the insurer's capacity to absorb risk with due regard to the nature, probability, duration, correlation, and potential severity of risks);

(d) gain and maintain an aggregated view of the risk profile of the insurer at a solo and, where relevant, at the group level;

(e) evaluate the internal and external risk environment on an on-going basis in order to identify and assess potential risks as early as possible;

(f) consider risks arising from remuneration arrangements and incentive structures;

(g) conduct regular stress testing and scenario analyses, including in respect of outliers or matters with low probability but high potential impact;

(h) regularly report to the managing executives, heads of 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;

(i) document and report material adverse changes affecting the insurer's risk management system to the board of directors to help ensure that the framework is maintained and improved; and

(j) conduct regular assessments of the risk management function and the risk management system and implement or monitor the implementation of any needed improvements.

(2) The risk management function must have access to and report to the board of directors on –

(a) the strategy of the risk management function;

(b) the risk management function's operational plan, including specific annual or other periodic goals being pursued and the performance against such goals;

(c) information on the risk management function's resources (such as personnel and budget) including an analysis on the appropriateness of these resources;

(d) an assessment of the insurer's risk profile and changes thereto;

(e) where appropriate, an assessment of pre-defined risk limits;

(f) where appropriate, risk management matters in relation to strategic affairs such as corporate strategy, mergers and acquisitions, and major projects and investments; and

(g) an assessment of risk events and the identification of appropriate remedial actions.

(3) The risk management function must promptly inform the board of directors of any circumstance that may have an adverse material effect on the risk management system of the insurer.

Compliance function

27. (1) The compliance function must establish, implement and maintain appropriate mechanisms and activities (including a strategy and compliance plan) to -

(a) promote and sustain an ethical corporate culture that values responsible conduct and compliance with internal and external obligations; this includes communicating and holding training on an appropriate code of conduct or similar that incorporates the corporate values of the insurer, aims to promote a high level of professional conduct of the business, and sets out the key conduct expectations of employees;

(b) identify, assess, report on, and address key legal and regulatory obligations and the risks associated therewith, including obligations under the Act;

(c) ensure the insurer does appropriate monitoring of and has appropriate policies, processes, and controls in respect of key areas of legal, regulatory, and ethical obligations;

(d) hold regular training on key legal and regulatory obligations particularly for employees in positions of trust or responsibility or who are involved in high risk activities;

(e) facilitate the confidential reporting by employees of concerns, shortcomings or potential violations in respect of insurer policies, legal or regulatory obligations, or ethical considerations;

(f) address compliance shortcomings and violations, including ensuring that adequate disciplinary actions are taken where appropriate and any necessary reporting to the Registrar or other regulatory authorities is made; and

(g) conduct regular assessments of the compliance function and the compliance policies and systems and implement or monitor needed improvements.

(2) The compliance plan must –

(a) promote the corporate culture and ethical values that underpin responsible compliance with internal and external obligations;

(b) identify all material legal and regulatory obligations and the risks associated therewith;

(c) document policies, processes, and controls in respect of all material compliance obligations;

(d) determine the processes and procedures for monitoring of all material compliance

obligations;

(e) determine the processes and procedures for ongoing training of relevant staff in respect of compliance obligations; and

(f) determine the processes and procedures for confidential reporting by employees of shortcomings or violations of compliance obligations.

(3) The compliance function must have access to and report to the board of directors on -

(a) the strategy of the compliance function;

(b) the compliance function's operational plan, including specific annual or other short-term goals being pursued and the performance against such goals;

(c) information on its resources (such as personnel and budget), including an analysis on the appropriateness of those resources;

(d) an assessment of the key compliance risks the insurer faces and the steps being taken to address them;

(e) an assessment of how the various parts of the insurer (such as divisions, major business units and product areas) are performing against compliance standards and goals;

(f) any compliance issues involving management or persons in positions of major responsibility within the insurer, and the status of any associated investigations or other actions being taken;

(g) material compliance violations or concerns involving any other person or unit of the insurer and the status of any associated investigations or other actions being taken; and

(h) material fines or other disciplinary actions taken by any regulatory authority in respect of the insurer or any employee.

(4) The compliance function must promptly inform the chair of the board of directors directly in the event of any major noncompliance by a member of management or a material non-compliance by the insurer with an external obligation if in either case he or she believes that managing executives or other persons in authority at the insurer are not taking the necessary corrective actions and a delay would be detrimental to the insurer or its policyholders.

Internal audit function

28. (1) The internal audit function must, at least, -

(a) provide independent assurance to the board of directors through general and specific audits, reviews, testing, and other techniques;

(b) establish, implement and maintain a risk-based audit plan to examine and evaluate

general or specific areas, including on a preventive basis;

(c) review and evaluate the adequacy and effectiveness of the insurer's policies and processes (including the reliability, integrity, and completeness of the accounting, financial reporting, and management information and IT systems) and the documentation and controls in respect of these, on a business unit, business area, department, or other organisational unit basis;

(d) review levels of compliance by employees and organisational units with established policies, processes, and controls, including those involving reporting;

(e) evaluate the reliability and integrity of information and the means used to identify, assess, classify, and report such information;

(f) ensure that the identified risks and the agreed actions to address them are accurate and current;

(g) evaluate the means of safeguarding insurer and policyholder assets (including fraud prevention, and misappropriation or misapplication of such assets) and, as appropriate, verify the existence of such assets and the required level of segregation in respect of insurer and policyholder assets;

(h) monitor and evaluate the effectiveness of the governance framework;

(i) monitor and evaluate the effectiveness of the insurer's risk management, compliance and actuarial functions;

(j) coordinate with the external auditors and, to the extent requested by the board of directors and not inconsistent with applicable law, evaluate the quality of performance of the external auditors; and

(k) conduct regular assessments of the internal audit function and audit systems and incorporate needed improvements.

(2) In carrying out the above tasks, the internal audit function must ensure that all material areas of risk and obligation of the insurer are subject to appropriate audit or review over a reasonable period of time, including, but not limited to -

(a) market, insurance, credit, liquidity, operational, and regulatory and compliance (including reputational) risk;

(b) accounting and financial policies and whether the associated records are complete and accurate;

(c) the extent of compliance by the insurer with applicable law, regulations, rules, and directives from all relevant jurisdictions;

(d) intra-group transactions, including intra-group risk transfer and internal pricing;

(e) adherence by the insurer to the insurer's remuneration policy;

(f) the reliability and timeliness of escalation processes and reporting systems, including whether there are confidential means for employees to report concerns or violations, and whether these are properly communicated, offer the reporting employee adequate protection from retaliation, and result in appropriate follow up; and

(g) the extent that any non-compliance with internal policies or external legal or regulatory obligations are documented, and appropriate corrective or disciplinary measures are taken, including in respect of individual employees involved.

(3) The internal audit function must have access to and, at least annually, report to the board of directors on -

(a) the strategy of the function;

(b) the function's audit plan, detailing the proposed areas of audit focus;

(c) an assessment on the extent of achievement of the goals set out in the audit plan;

(d) information on its resources;

(e) any factors that may impinge on the internal audit function's independence, objectivity, or effectiveness;

(f) material findings from audits or reviews conducted;

(g) material deficiencies of the internal control system, or of compliance with internal policies and procedures, and include recommendations to remedy all identified deficiencies; and

(h) the extent of management compliance with previously agreed upon corrective or risk mitigating measures.

Actuarial function

29. (1) The actuarial function must provide assurance to the board of directors regarding the accuracy of the calculations and the appropriateness of the assumptions underlying the insurance liabilities and the capital adequacy requirement, by, at least, performing the following functions:

(a) reviewing and attesting to the reliability and adequacy of the insurance liabilities and the capital adequacy requirement, including by -

(i) ensuring the appropriateness of the methodologies and underlying models used and assumptions made;

(ii) assessing the sufficiency and quality of the data used in the calculations;

(iii) comparing best estimates against experience when evaluating liabilities;

(iv) informing the board of directors of the reliability and adequacy of the calculations; and

(v) overseeing the calculations in the cases where, due to insufficient data of appropriate quality to apply reliable actuarial method, approximations were used in the calculation of liabilities and the capital adequacy requirement;

(b) expressing an opinion on the asset-liability management policy and the underwriting risk management policy;

(c) expressing an opinion on the reinsurance and other forms of risk transfer policy and the adequacy of reinsurance arrangements; and

(d) expressing an opinion on the actuarial soundness of premiums, benefits, and any other values thereof, including the awarding of bonuses to policyholders.

(2) Subsection (1) does not apply where the responsibilities and functions of the actuarial function are performed by the statutory actuary in terms of section 20 of the Long-term Insurance Act to the extent that these requirements are addressed in section 20.

Head of control function

30. (1) (a) An insurer, subject to paragraphs (b) and (c), must appoint a head for each of the control functions referred to in section 25(1), in respect of which no exemption was granted under section 25(2).

(b) 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.

(c) The appointment, annual or other periodic performance assessment and dismissal of the head of the internal audit function, and his or her remuneration, promotions, demotions or disciplinary actions must be done by the board of directors, its chairperson or the audit committee.

(2) (a) An insurer may, where appropriate in light of the nature, scale and complexity of the insurer's business and risks, appoint –

(i) a person as the head of more than one control function (other than the head of the internal audit function); or

(ii) the statutory actuary as the head of the actuarial function, if that appointment provides that the statutory actuary may not conduct any activities for the insurer which would compromise the independence and oversight requirements of the role of the actuarial function.

(b) An insurer may not outsource the head of control function in respect of the risk management function or the compliance function, without the approval of the Registrar.

(3) Despite subsection (2), the Registrar may direct the insurer to appoint another or a dedicated person as the head of that control function, if the Registrar is of the opinion that –

(a) that person is not a suitable head for more than one control function; or

(b) the appointment of that person as the head of more than one control function will detract from an adequate control environment and risk management system, taking into account the nature, scale and complexity of the business of the insurer and the risks to which it is exposed; or

(c) the appointment of the statutory actuary as the head of the actuarial function will detract from an adequate control environment and risk management system, taking into account the nature, scale and complexity of the business of the insurer and the risks to which it is exposed.

(4) The head of each control function must –

(a) regularly report to the board of directors or one of its committees;

(b) communicate directly and regularly meet (without the presence of managing executives) with the chairperson of the board of directors or one of its committees.

(5) The head of a control function must –

(a) without delay, report in writing to the board of directors any matter relating to the business of the insurer of which the head becomes aware in the performance of the functions and which, in the head's opinion, constitutes a contravention of any section of the Act or a material contravention of any other legislation that applies to the insurer; and

(b) where the matter relates to a contravention of the Act, submit the report referred to in paragraph (a), without delay to the Registrar if, in the opinion of the head, appropriate steps to rectify the matter are not taken by the board of directors to the satisfaction of the head within 30 days after the date in which the report was submitted to the board of directors.

PART 6: GENERAL

Title and commencement

31. This Notice is called the Notice on the Governance and Risk Management Framework for Insurers, 2014 and takes effect on 1 April 2015.

Transitional provisions

32. (a) The Registrar may where practicalities require the progressive application of a specific section of this Notice, exempt any insurer from that section for a specified period on specific conditions.

(b) A delay or exemption in terms of paragraph (a) may apply to insurers generally or be limited in application to particular kinds or types of insurers.