Solvency Assessment and Management: Pillar II – Sub Committee

Governance Task Group

Discussion Document 81 (v 3)

Governance, Risk Management, and Internal Controls – INTERIM REQUIREMENTS

CONTENTS

1. INTRODUCTION AND PURPOSE

Pending the finalisation of the Solvency Assessment and Management (SAM) project, the Financial Services Board (FSB) considers it essential to introduce interim measures to address shortcomings in respect of appropriate guidance on corporate governance, risk management and internal controls in the insurance sector.

The interim measures are intended to take effect in 2014.

The on-going financial soundness and stability of an insurer is highly dependent on the quality of its leadership, governance, and management teams, and on its risk management and internal control systems. It is therefore also vital that these interim measures prepare insurance and reinsurance companies (collectively referred to as “insurers” in this document) for the SAM regime. Ideally the interim measures should increase awareness of risk exposures, as well as improve the scrutiny and management of these matters.

The minimum standards set out in this document apply to all insurers. In some places, additional guidance is provided both for the sake of completeness and as an indication of voluntary best practice to be considered in the context of the nature, scale, and complexity of the insurer.

Governance framework recommendations should not present larger insurers with significant challenges; as such insurers should already have the majority of these measures in place. However, the FSB is concerned that not all insurers are meeting these fundamental governance standards. Currently, the Insurance Acts are somewhat silent as to governance requirements. It is the FSB’s experience that certain of the smaller insurers do not have appropriate governance in place to ensure that policyholders are adequately protected.

For this reason it has been found necessary to introduce certain interim governance requirements, as such measures cannot wait until the implementation of SAM in 2015. The Risk Management System interim measures focus on high level principles, rather than being too prescriptive with respect to the risk management methodology to be used. Many of the more detailed requirements in respect of the Risk Management System referred to by Solvency II and the International Association of Insurance Supervisors (IAIS) Insurance Core Principles (ICPs) can only be met once the quantitative requirements under SAM have been finalised. At this stage it is seen as too early to introduce particular risk management system concepts or risk taxonomy issues as this should be left to the final measures. Similarly, the level of detail on risk mitigation and reinsurance aspects is confined to high level principles.

It has however also been decided to provide insurers with some indication of concepts that will be dealt with in the final requirements by retaining these concepts in an annexure (Annexure G: Enterprise Risk Management), as guidance. Insurers should already be thinking about how they will implement these measures by 2015.

Many of the concepts presented in this framework are reflected across different sections, and are in many instances not fully developed to the extent that they are within the original source material. This format has been used for ease of comparison between the requirements in the jurisdictions surveyed. These concepts have been collated from the international standards prescribed by IAISICPs and relevant Solvency II Level I Directive and Level II Implementing Advice of the European Insurance and Occupational Pensions Authority (EIOPA). Existing governance requirements in the Australian Prudential Regulatory Authority (APRA) and Office of the Superintendent of Financial Institutions (OSFI) jurisdictions can be found in Annexure D. Regard has been given to the South African Banks Act, Companies Act, King III, and the CISNA Code. A list of references can be found in the appendix.

The proposed governance, risk management and internal controls interim requirements will be given effect through legislative changes, in the form of a planned Insurance Laws Amendment Bill (ILAB). Currently the Long-term and Short-term Insurance Acts,

respectively, contain very broad enabling provisions for governance and risk management in the primary legislation, specifically in section 9 (Application for registration) read with section 12 (Registrar may under certain circumstances prohibit long / short term insurers from carrying on business). The gist of these general provisions is that on application an insurer must have the organisation or management necessary and adequate for the carrying on of the business concerned, while section 12 requires this on an on-going basis.

More specific provisions in the current legislation applicable to governance and risk management are found in section 10 (Conditions of registration) read with section 28 (Maintenance of financially sound condition), section 16 (Head Office and Public Officer), section 17 (Financial Year), section 18 (Notification of certain appointments, terminations and resignations), section 19 (Auditor), section 20 (Statutory Actuary), section 23 (Audit Committee), section 26 (Limitation on control and certain shareholding or other interest in a long / short term insurer), and section 27 (Furnishing of information concerning shareholders).

Interim measures will become law once the planned ILAB is enacted; expected to be in January 2014. Once the proposals are near finalisation a decision will be made as to which should become effective immediately as against those which may require a transition period

In addition to these governance, risk management and internal control interim measures, the need has also been identified for interim measures in respect of insurance group supervision. This document does not specifically address the governance framework applicable to insurance groups, but some of the governance requirements for insurers on a solo entity basis can equally be applied to the non-operating holding company of the insurance group. Further reference can be made to the Insurance Groups Interim Measures Discussion Document 1, Version 10.

2. GOVERNANCE FRAMEWORK

2.1 General Governance Framework

2.1.1 IAIS ICP

ICP 7 High level principle

Insurers are required to establish and implement a corporate governance framework which provides for prudent management and oversight of the insurer's business operations and adequately protects the interests of policyholders.

ICP 7 Introduction:

Paragraph 7.0.1

Corporate governance refers to systems (such as structures, policies and processes) through which an entity is managed and controlled. Accordingly, the corporate governance framework of an insurer:

- promotes the development, implementation, and effective oversight of policies that clearly define and support the objectives of the insurer;
- defines the roles and responsibilities of persons accountable for the management and oversight of an insurer by clarifying who possesses legal duties and powers to act on behalf of the insurer and under which circumstances;
- sets requirements relating to how decisions and actions are taken including documentation of significant or material decisions, along with their rationale;

- provides for communicating, as appropriate, matters relating to the management, conduct and oversight of the insurer to stakeholders; and
- provides for corrective actions to be taken for noncompliance or weak oversight, controls or management.

Paragraph 7.0.2

Corporate governance is often referred to as a system of “checks and balances”. This recognises that an insurer has to be flexible and responsive to developments affecting its operations in making timely decisions, while at the same time being transparent and having appropriate systems, controls and limits to ensure that powers are not unduly concentrated and are used in the best interest of the insurer as a whole and its stakeholders.

Paragraph 7.0.3

Effective corporate governance supports and enhances the ability of the key players responsible for an insurer’s corporate governance; i.e. the insurer’s Board of Directors (“the Board"), Senior Management and Key Persons in Control Functions to manage the insurer’s business soundly and prudently. This allows the supervisor to place greater confidence in their work and judgement.

2.1.2 Solvency II Level I Directive

Article 41 - General governance requirements

1. Member States shall require all insurance and reinsurance undertakings to have in place an effective system of governance which provides for sound and prudent management of the business.

   That system shall at least include an adequate transparent organisational structure with a clear allocation and appropriate segregation of responsibilities and an effective system for ensuring the transmission of information. It shall include compliance with the requirements laid down in Articles 42 to 49.

   The system of governance shall be subject to regular internal review.

2. The system of governance shall be proportionate to the nature, scale and complexity of the operations of the insurance or reinsurance undertaking.

3. Insurance and reinsurance undertakings shall have written policies in relation to at least risk management, internal control, internal audit and, where relevant, outsourcing. They shall ensure that those policies are implemented.
   Those written policies shall be reviewed at least annually. They shall be subject to prior approval by the administrative, management or supervisory body and be adapted in view of any significant change in the system or area concerned.

4. Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, the undertaking shall employ appropriate and proportionate systems, resources and procedures.

5. The supervisory authorities shall have appropriate means, methods and powers for verifying the system of governance of the insurance and reinsurance undertakings and for evaluating emerging risks identified by those undertakings which may affect their financial soundness.

2.1.3 Solvency II Level II Implementing Advice

EIOPA CP 33 summary

The supervisor will evaluate the insurer's governance framework according to the following criteria. The insurer's system of governance must:

- Maintain effective cooperation, internal reporting, and communication of information;
- Have a clear and well-defined organisational structure;
- Ensure that the Board of Directors and Senior Management collectively possess sufficient professional qualifications, knowledge, and experience to provide prudent management of the insurer;
- Ensure personnel have the skills, knowledge, and expertise necessary to discharge their responsibilities;
- Ensure all personnel are aware of the procedures for the proper discharge of their responsibilities;
- Establish, implement, and maintain decision-making procedures;
- Ensure that the performance of multiple tasks by any individual does not create a legal or ethical conflict of interest;
- Establish and maintain adequate risk management, compliance, internal audit, and internal control functions;
- Ensure that each key function has an appropriate standing in terms of organisational structure;
- Internal Control Functions shall have direct access to the Board of Directors;
- Policies on governance, risk management, and internal control in respect of the Key Control Functions (being the Board of Directors and Senior Management), and in respect of the Key Internal Control Functions, shall clearly set out the relevant responsibilities, goals, processes, and reporting procedures to be applied.
- Establish information systems covering all business activities, the commitments assumed, and the risks to which the insurer is exposed;
- Maintain adequate and orderly records of its business and internal organisation;
- Safeguard the security, integrity, and confidentiality of information;
- Introduce clear reporting lines for the prompt transfer of information consistent with the importance of that information;
- Strive to identify any potential source of conflicts of interest and establish procedures to address these;
- Identify the risks for which contingency plans should be in place;
- Regularly test and update these plans.

2.1.4 Recommendation

Primary legislation:

Insurers are required to adopt and implement and document an effective governance framework that provides for the prudent management and oversight of their insurance business and adequately protects the interests of policyholders.

An insurer's governance framework must be proportionate to the nature, scale and complexity of the operations of the insurer.

At a minimum, the governance framework should provide for:

1. An adequate transparent organisational structure with a clear allocation and appropriate segregation of responsibilities;

2. Compliance with all requirements in respect of:

   - fit and proper requirements for directors, senior management and heads of control functions;
   - the risk management system;
   - the internal controls system;
   - control functions; and
   - outsourcing.

3. Written policies, approved by the Board of Directors, consistent with the requirements set out in section 3 - Risk Management System, section 4 - Internal Controls System, and section 5 - Outsourcing of this Discussion Document
   Note: All insurers will also be required to comply with the governance principles contained in the Companies Act 71 of 2008, whether or not the insurer is a company (appropriately modified for mutual insurers where necessary).

Some of the more detailed governance requirements, and the respective roles and responsibilities of the Board, Senior Management and Key Persons in Control Functions in this regard, are dealt with in the sections that follow. The FSB recognises that there are numerous frameworks and methodologies available both in South Africa and globally to design and implement a governance framework.[1] Insurers may consider a number of alternatives to achieve the same objective. Accordingly the FSB will not prescribe or favour a specific framework or methodology, but will rather monitor the outcome through its Prudential Risk Based Supervisory (RIBS) approach.

The substance of these frameworks and methodologies are elaborated upon and the interrelationships between them illustrated in ***Annexure A***.

3. BOARD OF DIRECTORS

3.1 Composition and governance of the Board of Directors

3.1.1 IAIS ICP

ICP Standard 7.3

The supervisor requires the insurer's Board to have, on an on-going basis:

- an appropriate number and mix of individuals to ensure that there is an overall adequate level of knowledge, skills and expertise at the Board level commensurate with the governance structure and the nature, scale and complexity of the insurer's business;
- appropriate internal governance practices and procedures to support the work of the Board in a manner that promotes the efficient, objective and independent judgement and decision making by the Board; and
- adequate powers and resources to be able to discharge its duties fully and effectively.

Paragraphs 7.3.1 through 7.3.3 summary

The Board should collectively and individually have, and continue to maintain, including through training, necessary skills, knowledge and understanding of the insurer's business to

[1] These frameworks include: the three lines of defence, segregation of duties, four eye's principle, and generally accepted risk principles (GARP). Methodologies include the COSO integrated framework and the combined assurance model from King III.

be able to fulfil their roles. In particular, the Board should have, or have access to, knowledge and understanding of areas such as the lines of insurance underwritten by the insurer, actuarial and underwriting risks, finance, accounting, the role of control functions, investment analysis and portfolio management and obligations relating to fair treatment of customers. While certain areas of expertise may lie in some but not all members, the collective Board should have an adequate spread and level of relevant competencies and understanding as appropriate to the insurer´s business.
Board members should meet the suitability requirements set out in ICP 5: Suitability of Persons and have the commitment necessary to fulfil their roles.
Board members should avoid commercial or business interests which conflict with that of the insurer.

Paragraph 7.3.4 excerpt

The Board should review, at least annually, its own performance to ascertain whether members collectively and individually remain effective.

Paragraph 7.3.8 summary

The Board should establish clear and objective independence criteria which should be met by a sufficient number of members of the Board to promote objectivity in decision making.

3.1.2 Solvency II Level II Implementing Advice

EIOPA CP 33

Ensure that the members of the administrative, management or supervisory body possess sufficient professional qualifications, knowledge and experience in the relevant areas of the business to give adequate assurance that they collectively are able to provide a sound and prudent management of the undertaking.

Undertakings shall ensure that at least two persons effectively run the undertaking [the four eye's principle].

3.1.3 Recommendation

Primary legislation:

- The Board should ensure that at all times: There are a sufficient number of non-executive and independent directors on the Board to promote objectivity in decision making by the Board.
- There is an appropriate number and mix of individuals to ensure that there is an overall adequate spread and level of knowledge, skills and expertise at the Board level commensurate with the nature, scale and complexity of the insurer's business and risks. The chairperson of the Board is an independent director.
- The chairperson of the Board cannot have been the CEO of the insurer at any time during the previous three years or currently.

Where the composition of the Board does not comply with the above recommendations, the insurer should report, and provide an explanation, to the Registrar as well as publicly disclose such explanation in its annual financial statements. Where the Registrar has concerns that the Board composition is such that the outcome of objectivity in decision-making is not achieved, the Registrar can require that the insurer appoint additional non-executive directors or independent directors.

The Board of the insurer must have appropriate internal governance practices and procedures to support the work of the Board in a manner that promotes the efficient, objective and independent judgement and decision making by the Board; and

The Board must have adequate powers and resources to discharge its duties fully and effectively.

The Board should adopt and implement a procedure to review, at least annually, the performance of the Board collectively, and of Board members individually.

Notes:

Board members should meet the suitability requirements set out in Annexure B - Fit and Proper Criteria and have the commitment necessary to fulfil their roles.

Given the objective of adequate policyholder protection, insurers will be subject to a certain requirements relating to Board composition that go beyond the requirements of the Companies Act. Accordingly, some aspects of King III are to be entrenched in insurance legislation (King III recommendations with respect to Board composition and a review of the provisions of the Companies Act can be found in Annexure H):

- A non-executive director is an individual who is not involved in the day-to-day management of the insurer.

- An independent director is a non-executive director who is free from any business or other association that could materially interfere with the exercise of their independent judgement.

3.2 Structure of the Board of Directors

3.2.1 Solvency II Level II Implementing Advice

Paragraphs 7.3.6 and 7.3.7 summary

The Chair of the Board has the pivotal role of providing leadership to the Board for its proper and effective functioning. The role of the Chair of the Board should generally encompass oversight over the Board and responsibilities such as setting the Board's agenda, ensuring that there is adequate time allocated for the discussion of agenda items, and for promoting a culture of openness and debate.

The Board should assess whether the establishment of committees of the Board is appropriate.

3.2.2 Recommendation

Primary legislation:

The Board must assess whether, and to what extent, the establishment of committees of the board is necessary and appropriate, subject to, at least establishing an Audit Committee (despite the provisions of the Companies Act).

If the Board elects not to establish a Risk Committee or Remuneration Committee, the board of directors must notify and motivate the non-establishment of that separate committee to the Registrar, and publically disclose and motivate the non-establishment of that separate committee

along with the insurer's annual financial statements.

Secondary legislation:

The Registrar may prescribe in subordinate legislation the functions of the Risk Committee, Remuneration Committee and Audit Committee (in addition to the functions prescribed in section 94 of the Companies Act).

Many of the specific oversight functions outlined in the ICP guidance are already provided for in section 94 of the Companies Act. Consideration will be given to whether specific functions over and above the functions prescribed in section 94 of the Companies Act will need to be prescribed for insurers, taking into account the objective of policyholder protection and the recommendations of King III – Principle 3.1.

Consideration will be given to the specific functions of the Risk Committee that need to be prescribed, taking into account the objective of policyholder protection and the recommendations of King III.

3.3 The Audit Committee

3.3.1 Solvency II Level II Implementing Advice

Paragraphs 7.3.6 and 7.3.7 summary

The Chair of the Board has the pivotal role of providing leadership to the Board for its proper and effective functioning. The role of the Chair of the Board should generally encompass oversight over the Board and responsibilities such as setting the Board's agenda, ensuring that there is adequate time allocated for the discussion of agenda items, and for promoting a culture of openness and debate.

The Board should assess whether the establishment of committees of the Board is appropriate.

Paragraph 7.7.1 excerpt

In discharging its responsibilities with respect to the financial reports of the insurer, the Audit Committee should carry out specific oversight functions. These functions should include:

- overseeing the financial statements, financial reporting, and disclosure processes;
- monitoring whether accounting policies and practices of the insurer are operating as intended;
- overseeing the audit process and reviewing the external auditor's plans and material findings;
- overseeing the processes for hiring, removing, and assessing the performance and independence of the external auditor;
- investigating the circumstances relating to the resignation or removal of an external auditor, and ensuring prompt actions are taken to mitigate any identified risks to the integrity of the financial reporting process; and
- reporting to the Board of Directors by the Audit Committee and the supervisor on any significant issues concerning the financial reporting process.

3.3.2 Recommendation

Primary legislation:

The Board, despite the Companies Act, must appoint at least three of its members to form and serve on an audit committee.

None of these members may be persons that are employees of the insurer or any of its related parties.

The chairperson of the Board or the insurer's controlling company may not be appointed as a member of the audit committee.

The chairperson of the audit committee may not be an employee of any related party of the insurer.

The insurer may apply to the Registrar for exemption from one or more of these requirements.

Secondary legislation:

The Registrar may prescribe in subordinate legislation the functions of the Audit Committee (in addition to the functions prescribed in section 94 of the Companies Act).

Section 23 of the Long-term Insurance Act and Section 22 of the Short-term Insurance Act currently contain provisions with respect to the functions of the Audit Committee. It is proposed that these be deleted and that functions of the Audit Committee, over and above the functions prescribed in section 94 of the Companies Act, may be prescribed by the Registrar in subordinate legislation.

Many of the specific oversight functions outlined in the ICP guidance are already provided for in section 94 of the Companies Act. Consideration will be given to whether specific functions over and above the functions prescribed in section 94 of the Companies Act will need to be prescribed for insurers, taking into account the objective of policyholder protection and the recommendations of King III – Principle 3.1.

3.4 Duties of each director

3.4.1 IAIS ICP

ICP Standard 7.4

The supervisor requires the individual members of the Board to:

- act in good faith, honestly and reasonably;
- exercise due care and diligence;
- act in the best interests of the insurer and policyholders, putting those interests of the insurer and policyholders ahead of his/her own interests;
- exercise independent judgement and objectivity in his/her decision making, taking due account of the interests of the insurer and policyholders; and
- not use his/her position to gain undue personal advantage or cause any detriment to the insurer.

Paragraph 7.3.3

Board members should avoid commercial or business interests which conflict with that of the insurer. Where it is not reasonably possible to avoid conflicts of interests, such conflicts

should be effectively managed. Procedures should be in place to address conflicts of interests which could include disclosure of potential conflicts of interests, requirements for arm's length transactions, and where appropriate, prior approval by the Board or shareholders of such transactions.

3.4.2 Recommendation

Primary legislation:

Section 76 of the Companies Act already adequately deals with individual Board member's duties with respect to acting in good faith, honestly and reasonably, and exercising due care and diligence. The following provision in the primary legislation, to require specific consideration of policyholder interests, is therefore proposed:

Individual members of the Board must, in addition to the requirements under section 76 of the Companies Act:

- act in the best interests of the insurer and policyholders, putting those interests of the insurer and policyholders ahead of their own interests; and
- exercise independent judgement and objectivity in their decision making, taking due account of the interests of the insurer and policyholders.

Further, individual members of the board must at all times meet the fit and proper requirements.

3.5 Roles and responsibilities of the Board of Directors

3.5.1 IAIS ICP

ICP 5 High level principle

The supervisor requires Board Members, Senior Management, Key Persons in Control Functions and Significant Owners of an insurer to be and remain suitable to fulfil their respective roles.

ICP Standard 7.1:

The supervisor requires the insurer's Board to set and oversee the implementation of, the insurer's business objectives and strategies for achieving those objectives, including its risk strategy and risk appetite, in line with the insurer's long-term interests and viability.

Paragraphs 7.1.1 through 7.1.4 summary

The Board should approve and implement business objectives and risk strategies, taking into account the long-term financial safety and soundness of the insurer as a whole, and the legitimate interests of its stakeholders, including fair treatment of customers.

The Board should approve the fundamental corporate values for the insurer which should be reflected in the insurer's business objectives and strategies, and be supported by professional standards and codes of ethics;

The Board should ensure that the insurer's overall business objectives and strategies are reviewed at least annually;

The Board should establish clear and objective performance goals and measures, both for the insurer and its Senior Management;

ICP Standard 7.2:

The supervisor requires the insurer's Board to:

- ensure that the roles and responsibilities allocated to the Board, Senior Management and Key Persons in Control Functions are clearly defined so as to promote an appropriate separation of the oversight function from the management responsibilities; and
- provide adequate oversight of the Senior Management.

Paragraphs 7.2.1 through 7.2.4 summary

The Board should ensure that the insurer has a well-defined governance structure which provides for the effective separation between oversight and management functions.

The Board should also ensure that there is a clear allocation of roles and responsibilities to the Board as a whole, to committees of the Board, and to the Senior Management and Internal Control Functions.

The allocation of responsibilities to individual Board members should take due account of whether the relevant member has the degree of independence and objectivity required to carry out the functions of the particular committee.

In order to provide effective oversight of the Senior Management, the Board should:

- ensure that there are adequate policies and procedures relating to the engagement, dismissal, and succession of the Senior Management;
- monitor whether the Senior Management is managing the affairs of the insurer in accordance with the strategies and policies set by the Board; and
- regularly meet with the Senior Management.

The Board should review whether the policies and procedures, as set by the Board, are being properly implemented.

Paragraph 7.3.11 summary

The Board may delegate some of the activities or tasks associated with its own roles and responsibilities, given that:

- there is an appropriate process for delegation of authority from the Board of Directors to Senior Management, and throughout all levels of the organisation.
- the delegation is appropriate;
- the delegation is made under a clear mandate;
- there is no undue concentration of powers;
- it has the ability to monitor and require reports on delegated tasks;
- it retains the ability to withdraw the delegation; and
- it retains responsibility and accountability for the outcomes of any delegation.

ICP Standard 7.5:

The supervisor requires the insurer's Board to provide oversight in respect of the design and implementation of sound risk management and internal control systems and functions.

Paragraph 7.5.1 excerpt

It is the Board's responsibility to ensure that the insurer has appropriate systems and functions for risk management and overall internal controls, and to provide oversight to ensure that these systems and the functions that oversee them are operating effectively and as intended.

ICP Standard 7.6:

The supervisor requires the insurer's Board to:

- adopt and oversee the effective implementation of a remuneration policy, which does not induce excessive or inappropriate risk taking, is in line with the identified risk appetite and long-term interests of the insurer, and has proper regard to the interests of its stakeholders; and
- ensure that such a remuneration policy, at a minimum, covers those individuals who are members of the Board, Senior Management, Key Persons in Control Functions and other employees whose actions may have a material impact on the risk exposure of the insurer ("major risk–taking staff").

ICP Standard 7.7:

The supervisor requires the insurer's Board to ensure there is a reliable financial reporting process for both public and supervisory purposes which is supported by clearly defined roles and responsibilities of the Board, Senior Management and the external auditor.

Paragraph 7.7.2 excerpt

To promote and maintain an effective relationship with the external auditor the Board of Directors should ensure that:

- the terms of engagement of the external auditor are clear and appropriate to the scope of the audit and resources required to conduct the audit, and specify the level of audit fees to be paid;
- the external auditor undertakes a specific responsibility under the terms of engagement to perform the audit in accordance with applicable auditing standards;
- there are adequate policies and a process to ensure the independence of the external auditor;
- there is adequate dialogue with the external auditor on the scope and timing of the audit to understand the issues of risk, information on the insurer's operating environment which is relevant to the audit, and any areas in which the Board may request for specific procedures to be carried out by the External Auditor, whether as part or extension of the audit engagement;

Paragraphs 7.7.3 through 7.7.7 summary

The Board should also understand the External Auditor's approach to internal controls relevant to the audit. This includes evaluating the relationship between the External Auditor, the Internal Audit Function, and the Actuarial Function in order to establish the degree of assurance that the Board can draw from the External Auditor's report.

There should be regular meetings between the Board and the External Auditor during the audit cycle, including meetings without management present.

The Board should ensure that significant findings and observations regarding weaknesses in the financial reporting process are promptly rectified. This should be supported by a formal process for reviewing and monitoring the implementation of recommendations by the external auditor.

ICP Standard 7.8:

The supervisor requires the insurer's Board to have systems and controls to ensure the promotion of appropriate, timely and effective communications with the supervisor and relevant stakeholders on the governance of the insurer.

ICP Standard 7.9:

The supervisor requires the insurer's Board to have appropriate policies and procedures to ensure that the Senior Management:

- carries out the day-to-day operations of the insurer effectively and in accordance with the insurer's strategies, policies and procedures;
- promotes a culture of sound risk management, compliance and fair treatment of customers;
- provides the Board adequate and timely information to enable the Board 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 the Senior Management; and
- provides to the relevant stakeholders and the supervisor the information required to satisfy the legal and other obligations applicable to the insurer or the Senior Management.

Paragraph 7.10.1

The supervisor plays an important role by requiring the Board and Senior Management of the insurer to demonstrate that they are meeting the applicable corporate governance requirements, consistent with these Standards, on an on-going basis. For this purpose, the supervisor should assess whether the insurer's overall corporate governance framework, including remuneration policies and practices, is effectively implemented and remains adequate by undertaking periodic on-site inspections and/or other (including offsite) reviews as appropriate to the nature, scale and complexity of the insurer's business and its risk profile. Where significant changes in the insurer's corporate governance framework are identified, including through information provided by the insurer, the supervisor should update its assessment.

Paragraph 7.10.3

The supervisor should assess the effectiveness of the Board, particularly whether the Board members have the relevant expertise, ability and commitment among them to provide effective leadership, direction and oversight of the insurer, taking into due account of the nature scale and complexity of operations of insurer. The supervisory review should encompass the expertise and qualifications of Board members, their continuous training, the frequency of their participation and proactive involvement in Board proceedings as evidenced by the minutes or records of such meetings and the quality and timeliness of the information made available to Board members relating to the affairs of the insurer including for the purposes of the Board or committee meetings.

3.5.2 Solvency II Level II Implementing Advice

EIOPA CP 33

An effective risk management system requires... [a] clearly defined and well documented risk management strategy that includes the risk management objectives, key risk management principles, general risk appetite and assignment of risk management responsibilities across all the activities of the undertaking and is consistent with the undertaking's overall business strategy.

The policies on risk management, internal control, internal audit and, where relevant, outsourcing, shall clearly set out the relevant responsibilities, goals, processes and reporting procedures to be applied, all of which shall be in line with the undertaking's overall business strategy.

EIOPA CP 59

An overall remuneration policy and practice that is in line with the insurer's business and risk strategy, risk profile, objectives, values, risk management practices, and long-term entity-wide interests and performance shall be adopted.

3.5.3 Recommendation

Primary legislation:

The insurer's Board of Directors must determine and oversee the implementation of the insurer's business objectives, and strategies for achieving those objectives, consistent with the insurer's long-term interests and viability and the legitimate interests of its stakeholders.

The Board of Directors is required to ensure that the roles and responsibilities allocated to the Board, Senior Management, and Key Control Functions are clearly defined so as to promote an appropriate separation of the oversight function from the management responsibilities

The Board of Directors must ensure that there are adequate policies and procedures relating to the appointment, dismissal and succession of Senior Management.

The Board of Directors is responsible for monitoring Fit and Proper requirements on an on-going basis to facilitate the sound and prudent management of the business of the insurer.

Note: Fit and proper means that Board Members, Senior Management, and Key Persons in Control Functions must have the competence and integrity to fulfil their respective roles, and Shareholders Deemed to Exercise Control must have the soundness and integrity to fulfil their roles.

These criteria may be found in Annexure B.

The Board of Directors must provide oversight in respect of the design and implementation of sound risk management and internal controls systems and functions.

The Board must adopt and oversee the effective implementation of policies and procedures.

The Board of Directors is responsible for ensuring reliable and transparent financial reporting for public and supervisory purposes.

The insurer's Board of Directors is required to adopt and implement systems and controls to ensure the promotion of appropriate, timely, and effective communications with the supervisor and relevant stakeholders on the governance of the insurer, which allow informed judgements to be made about the effectiveness of the Board of Directors and Senior Management in governing the insurer.

The insurer's Board of Directors should adopt and implement appropriate policies and procedures to ensure that the Senior Management:

- carries out the day-to-day operations of the insurer effectively and in accordance with the insurer's strategies, policies, and procedures;
- promotes a culture of sound risk management, compliance and policyholder protection;
- provides the Board with adequate and timely information to enable the Board 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 the Senior Management; and
- provides to the relevant stakeholders and the supervisor the information required to satisfy the legal and other obligations applicable to the insurer or the Senior Management.

The Board of Directors must regularly monitor and evaluate the adequacy and effectiveness of the governance framework.

The Board may delegate some of the activities or tasks associated with its own roles and responsibilities, given that:

- there is an appropriate process for delegation of authority from the Board of Directors to Senior Management, and throughout all levels of the organisation.
- the delegation is made under a clear mandate;
- there is no undue concentration of powers;
- it has the ability to monitor and require reports on delegated tasks;
- it retains the ability to withdraw the delegation; and
- it retains responsibility and accountability for the outcomes of any delegation.

Irrespective of whether the Board has delegated its roles and responsibilities, an omission or act done by the delegated party shall be deemed to have been done by the board its self.

Subordinate legislation:

The supervisor may at its discretion require the Board of Directors and Senior Management of the insurer to demonstrate that they are meeting the applicable governance requirements,

The Board of Directors should ensure that an evaluation of the effectiveness of the external audit process at the end of the audit cycle is performed.

There must be unrestricted access by the External Auditor to information and persons within the insurer as necessary to conduct the audit.

There should be regular meetings between the Board and the External Auditor during the audit cycle, including meetings without management present.

The Board should ensure that significant findings and observations regarding weaknesses in the financial reporting process are promptly rectified. This should be supported by a formal process for reviewing and monitoring the implementation of recommendations by the external auditor.

The allocation of responsibilities to individual Board members should take due account of whether the relevant member has the degree of independence and objectivity required to carry out their allocated functions.

Additional Guidance:

The Board should approve the fundamental corporate values for the insurer, which should be reflected in the insurer's business objectives and strategies, and be supported by professional standards and codes of ethics;

The Board should ensure that the insurer's overall business objectives and strategies are reviewed at least annually.

The roles and responsibilities identified as minimum standards above should be incorporated into the Board charter or mandate containing the terms of engagement of the individual Board members.

To promote and maintain an effective relationship with the external auditor the Board of Directors should ensure that:

- the terms of engagement of the External Auditor are clear and appropriate to the scope of the audit and resources required to conduct the audit, and specify the level of audit fees to be paid;
- the External Auditor undertakes a specific responsibility under the terms of engagement to perform the audit in accordance with applicable auditing standards;
- there are adequate policies and a process to ensure the independence of the External Auditor;
- there is adequate dialogue with the external auditor on the scope and timing of the audit to understand the issues of risk, information on the insurer's operating environment which is relevant to the audit, and any areas in which the Board may request for specific procedures to be carried out by the External Auditor, whether as part or extension of the audit engagement;
- The Board should also understand the External Auditor's approach to internal controls relevant to the audit. This includes evaluating the relationship between the External Auditor, the Internal Audit Function, and the Actuarial Function in order to establish the degree of assurance that the Board can draw from the External Auditor's report.

The supervisor may wish to assess whether the insurer's overall governance framework is effectively implemented and remains adequate and appropriate to the nature, scale, and complexity of the insurer's business and its risk profile by undertaking periodic on-site inspections or offsite reviews.

As part of such an assessment, the supervisor would wish to evaluate the effectiveness of the Board in respect of their collective expertise, ability, and commitment to provide effective leadership, direction, and oversight of the insurer, taking due account of the nature, scale, and complexity of operations of the insurer.

4. THE RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS

4.1 The risk management system

4.1.1 IAIS ICP

ICP Standard 8.1

The Supervisor requires an insurer to establish, and operate within, an effective system of risk management and of internal controls, including effective functions for risk management, compliance, actuarial matters, and internal audit.

Paragraph 8.0.1

As part of the overall corporate governance framework and in furtherance of the safe and sound operation of the insurer, the Board of Directors is responsible for overseeing that (a) the insurer has in place effective systems and functions to address the key risks it faces and for the key legal and regulatory obligations that apply to it and (b) Senior Management

implements these systems properly and provides the necessary resources and support for these functions.

Paragraphs 8.0.1 through 8.0.4 summary

The risk management system of an insurer comprises the totality of strategies, policies, and procedures for identifying, measuring, monitoring, managing, and reporting risks to which the insurer may be exposed at an individual and at a consolidated level.

The risk management system should be adequate for the nature, scale, and complexity of the insurer's business and risks, and should be adapted as the insurer's business and the external environment change.

Paragraphs 8.1.2 through 8.1.3

The risk management system is designed and operated to identify, assess, monitor, manage and report on all reasonably foreseeable material risks of the insurer in a timely manner. It takes into account the probability, potential impact, and time duration of risks.

While subject to the principle of proportionality, the risk management system should include at least the following elements:

- 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);
- relevant objectives, key principles, and proper allocation of responsibilities for dealing with risk across the business areas and organisational units of the insurer, including branches;
- a clearly defined risk appetite approved by the Board;
- a written process defining the Board approval required for any deviations from the risk management strategy or the risk appetite and for settling any major interpretations issues thereunder;
- appropriate written policies that include a definition and categorisation of the material risks (by type) to which the insurer is exposed, and the levels of acceptable risk limits for each type of risk (such as underwriting, market, credit, liquidity, operational, and reputational risk, but also internal risks such as those arising from intra-group or related party pricing, transfers, transactions, etc.). These policies define the risk standards and the specific obligations of employees and the businesses in dealing with risk, including in respect of capital, risk escalation and risk mitigation (e.g. reinsurance, hedging);
- appropriate processes and tools (including, where appropriate, models) for identifying, assessing, monitoring, managing, and reporting on risks. Such processes should also cover areas such as contingency planning, business continuity, and crisis management;
- regular reviews of the risk management system (and its components) to help ensure that necessary modifications and improvements are identified and made in a timely manner;
- appropriate attention to other matters set out in ICP 16 on Enterprise Risk Management for Solvency.
- an effective risk management function.

Paragraphs 8.1.4 through 8.1.12

The risk management system should take into account relevant local or business specific risks as well as enterprise-wide risks. This includes current and emerging risks.

The risk management system should be integrated into the culture of the insurer and into the various business areas and units of the insurer.
The insurer's risk policies should be written in a way to help employees understand their risk responsibilities.
Regular communications and training on the risk policies should take place.
The insurer's risk escalation process should allow for reporting on risk issues within established reporting cycles and outside of them for matters of particular urgency.
The Board should have appropriate ways to carry out its responsibilities for risk oversight. This includes having a policy on the content, form, and frequency of reporting that it expects on risk from (a) Senior Management and (b) each of the Internal Control Functions.
Significant new activities and products of the insurer that may increase an existing risk or create a new type of exposure should be subject to appropriate risk review and approvals.
Both the Board and Senior Management should be attentive to the potential need to modify the risk management system in light of new internal or external circumstances.
Material changes to an insurer's risk management system should be documented and subject to approval by the Board.

ICP Standard 16.2

The supervisor requires the insurer's measurement of risk should be supported by accurate documentation providing appropriately detailed descriptions and explanations of the risks covered, the measurement approaches used, and the key assumptions made.

4.1.2 Solvency II Level I Directive

Article 44 - Risk management

1. Insurance and reinsurance undertakings shall have in place an effective risk-management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies. That risk-management system shall be effective and well integrated into the organisational structure and in the decision-making processes of the insurance or reinsurance undertaking with proper consideration of the persons who effectively run the undertaking or have other key functions.

2. The risk-management system shall cover the risks to be included in the calculation of the Solvency Capital Requirement as set out in Article 101(4) as well as the risks which are not or not fully included in the calculation thereof. The risk-management system shall cover at least the following areas:
   (a) underwriting and reserving;
   (b) asset–liability management;
   (c) investment, in particular derivatives and similar commitments;
   (d) liquidity and concentration risk management;
   (e) operational risk management;
   (f) reinsurance and other risk-mitigation techniques.

   The written policy on risk management referred to in Article 41(3) shall comprise policies relating to points (a) to (f) of the second subparagraph of this paragraph.

   As regards investment risk, insurance and reinsurance undertakings shall demonstrate that they comply with Chapter VI, Section 6.

4.1.3 Solvency II Level II Implementing Advice

EIOPA CP 33

An effective risk management system requires at least the following:

- a clearly defined and well documented risk management strategy that includes the risk management objectives, key risk management principles, general risk appetite, and assignment of risk management responsibilities across all the activities of the insurer, and is consistent with the insurer's overall business strategy;
- adequate written policies that include a definition and categorisation of the material risks faced by the insurer, implement the insurer's risk strategy, facilitate control mechanisms and take into account the nature, scope, and time horizon of the business and the risks associated with it;
- appropriate processes and procedures which enable the insurer to identify, measure, manage, monitor, and report the risks it is or might be exposed to;
- appropriate reporting procedures and feedback loops that ensure that information on the risk management system, which is coordinated and challenged by the risk management function, is actively monitored and managed by all relevant staff and the administrative, management or supervisory body;
- reports that are submitted to the administrative, management or supervisory body by the risk management function on the material risks faced by the insurer and on the effectiveness of the risk management system; and
- a suitable own risk and solvency assessment (ORSA) process.

4.1.4 Recommendation

Primary legislation:

Insurers are required to establish and maintain an effective risk management system as part of their overall governance framework. The risk management system of an insurer should comprise the totality of resources, strategies, policies, and procedures for identifying, measuring, monitoring, managing, and reporting of all material risks to which the insurer may be exposed.

The risk management system must be capable of supporting the Board of Directors in its responsibilities with respect to the furtherance of the safe and sound operation of the insurer and the protection of policyholders.

The risk management system should be adequate for the nature, scale, and complexity of the insurer's business and risks, and should be adapted as the insurer's business and the external environment change.

The risk management strategy should include the risk management objectives, risk management principles and approach to assumption setting, and assignment of risk management responsibilities across all the activities of the insurer, consistent with the insurer's overall business strategy.

The risk management system must include adequate written policies consistent with the risk management strategy.

The risk management system should comprise appropriate processes, procedures and tools (including, where appropriate, models) for identifying, assessing, monitoring, managing, and reporting on material risks.

Reports to inform senior management and the Board of Directors on all material risks faced by the insurer and on the effectiveness of the risk management system itself should form part of the risk management system.

The risk management system should also include processes for ensuring adequate contingency planning, business continuity and crisis management.

The risk management system (and its components) must be reviewed regularly to help ensure that necessary modifications and improvements are identified and made in a timely manner. The Board of Directors should satisfy itself as to the capacity of Internal Audit to effectively carry out this review. If the Internal Audit function lacks the independence to perform this review an external party should be brought in to do so.

Any changes to an insurer's risk management system should be documented and subject to approval by the Board.

Note: Enterprise Risk Management (ERM) and the Own Risk and Solvency Assessment (ORSA) are not required to be implemented for the interim measures.

Secondary legislation:

Criteria for judging the effectiveness of risk management systems may be issued by means of Board Notice:

- The risk management system should be integrated into the culture of the insurer and into the various business units of the insurer.
- The risk management policies and procedures should be embedded within the organisational culture, consistent with the insurer's long-term strategy, and form an integral part of the insurer's risk management system. The risk management system should take into account both business specific risks and enterprise-wide risks, including current and emerging risks.
- The insurer's risk escalation process should establish procedures both for reporting on risk issues within normal reporting cycles and on an ad hoc basis to address matters of particular urgency.
- The Board of Directors should adopt and implement a policy on the content, form, and frequency of risk reports that it expects from Senior Management and each of the Key Control Functions.
- Written risk policies (referred to in section 5) below should be both accessible and understandable to relevant employees, and regular communications and training on these policies should take place.

Both the Board and Senior Management should be attentive to the potential need to modify the risk management system in light of changes in the internal or external circumstances of the insurer.

Documentation of the risk management system should meet minimum standards prescribed by the Registrar.

Documentation of the risk management system should include as a minimum:

- a definition and categorisation of the material risks to which the insurer is exposed pre and post risk mitigating steps,
- the levels of acceptable risk limits for each type of risk,

- Implementation of the insurer's risk strategy,
- facilitation of control mechanisms,
- the nature, scope, and time horizon of the business and the risks associated with it;
- defining the risk standards and the specific obligations of employees and the businesses in dealing with risk, including in respect of capital, risk escalation, and risk mitigation; and
- how risks are measured, and assumptions made in their measurement.

4.2 Risk management policies

4.2.1 IAIS ICP

ICP 13 High level principle

The supervisor sets standards for the use of reinsurance and other forms of risk transfer, ensuring that insurers adequately control and transparently report their risk transfer programmes.

ICP Standards 16.4, 16.5, 16.6, and 16.7

The insurer's Risk Management Policy should outline how all relevant and material categories of risk are managed, both in the insurer's business strategy and its day-to-day operations.

The insurer's Risk Management Policy should describe the relationship between the insurer's tolerance limits, regulatory capital requirements, economic capital, and the processes and methods for monitoring risk.

The insurer's Risk Management Policy should include an explicit asset-liability management (ALM) policy which clearly specifies the nature, role, and extent of ALM activities, and their relationship with product development, pricing functions, and investment management.

The insurer's Risk Management Policy should incorporate an explicit Investment Policy which:

- specifies the nature, role and extent of the insurer's investment activities.
- establishes 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.

The insurer's Risk Management Policy should include explicit policies in relation to underwriting risk.

4.2.2 Solvency II Level I Directive

Article 132 (Prudent Person Principle) extract

With respect to the whole portfolio of assets, insurance and reinsurance undertakings shall only invest in assets and instruments whose risks the undertaking concerned can properly identify measure, monitor, manage, control and report.

Assets held to cover the technical provisions shall also be invested in a manner appropriate to the nature and duration of the insurance and reinsurance liabilities. Those assets shall be invested in the best interest of all policy holders and beneficiaries taking into account any disclosed policy objective.

In the case of a conflict of interest, insurance undertakings, or the entity which manages their asset portfolio, shall ensure that the investment is made in the best interest of policy holders and beneficiaries.

4.2.3 Solvency II Level II Implementing Advice

EIOPA CP 33

An effective risk management system requires at least the following:

- a clearly defined and well documented risk management strategy that includes the risk management objectives, key risk management principles, general risk appetite, and assignment of risk management responsibilities across all the activities of the insurer, and is consistent with the insurer's overall business strategy;
- adequate written policies that include a definition and categorisation of the material risks faced by the insurer, implement the insurer's risk strategy, facilitate control mechanisms and take into account the nature, scope, and time horizon of the business and the risks associated with it;
- appropriate processes and procedures which enable the insurer to identify, measure, manage, monitor, and report the risks it is or might be exposed to;
- appropriate reporting procedures and feedback loops that ensure that information on the risk management system, which is coordinated and challenged by the risk management function, is actively monitored and managed by all relevant staff and the administrative, management or supervisory body;
- reports that are submitted to the administrative, management or supervisory body by the risk management function on the material risks faced by the insurer and on the effectiveness of the risk management system; and
- a suitable own risk and solvency assessment (ORSA) process.

Insurers should have adequate procedures and processes for the selection of suitable reinsurance programs, 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 mitigation technique used.

The insurer's reinsurance management strategy should incorporate the following considerations:

- identification of the level of risk transfer appropriate to the insurer's approach to risk;
- types of reinsurance arrangements most appropriate to limit risks to the insurer's insurance risk profile;
- principles for the selection of reinsurance counterparties;
- procedures for assessing the creditworthiness and diversification of reinsurance counterparties;
- procedures for assessing the effective risk transfer;
- concentration limits for credit risk exposure to reinsurance counterparties and appropriate systems for monitoring these exposures; and
- liquidity management to deal with any timing mismatch between claims' payments and reinsurance recoveries.

4.2.4 Recommendation

Primary legislation:

Insurers must develop and regularly review adequate written risk management policies that include a definition and categorisation of the material risks to which the insurer is exposed, taking into account the nature, scope, and time horizon of the insurance business, and the levels of acceptable risk limits for each type of risk.

The Risk Management Policy must incorporate an explicit Investment Policy and Remuneration Policy which should meet minimum requirements as prescribed by the Registrar.

Insurers must have at least the following policies –

- an explicit asset-liability management policy that clearly specifies the nature, role and extent of the insurer's asset-liability management activities and their relationship with product development, pricing functions and investment management;
- an explicit investment policy that –
  - provides for the investment of all the insurer's assets in accordance with the legislation
  - specifies the nature, role and extent of the insurer's investment activities and how the insurer complies with the regulatory investment requirements as prescribed the Registrar;
  - establishes 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; and
- an explicit reinsurance and other forms of risk transfer policy that –
  - outlines 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;
  - ensures 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;
  - provides for processes and procedures for ensuring that strategies are implemented and complied with, and that the insurer has in place appropriate systems and controls over its risk transfer transactions;
- an explicit remuneration policy that –
  - does not induce excessive or inappropriate risk taking, is consistent with the identified risk appetite and long-term interests of the insurer, and has proper regard to the interests of its stakeholders;
  - at a minimum, addresses directors, senior management, heads of control functions and other persons whose actions may have a material impact on the risk exposure of the insurer;
- explicit policies in relation to underwriting risk;
- an explicit insurance fraud risk management policy that –
  - outlines appropriate strategies, procedures and controls to deter, prevent, detect, report and remedy insurance fraud, and the effective manage fraud risk and possible risks to its financial soundness or continuity caused by fraud;
  - provides for the prompt reporting of insurance fraud to relevant regulatory authorities; and
- in respect of long-term insurers, an explicit anti-money laundering and combating the financing of terrorism management policy that –
  - outlines appropriate strategies, procedures and controls to deter, prevent, detect, report and remedy anti-money laundering and the financing of terrorism;
  - provides for the prompt reporting of anti-money laundering and the financing of terrorism to relevant regulatory authorities in accordance with legislative requirements.

Secondary legislation:

An insurer's Investment Policy should:

- take into account the Code for Responsible Investing by Institutional Investors in South Africa which was issued by the Committee on Responsible Investing by Institutional Investors in South Africa.
- adhere to the 'Prudent Person Principle':

- insurers should only invest in assets and instruments whose risks the organisation can properly identify measure, monitor, manage, control, and report.
- assets should be invested in a manner appropriate to the nature and duration of the insurers liabilities. Assets should be invested in the best interest of all policy holders and beneficiaries.

The insurer's reinsurance strategy should incorporate the following considerations:

- identification of the level of risk transfer appropriate to the insurer's approach to risk;
- types of reinsurance arrangements most appropriate to limit risks to the insurer's insurance risk profile;
- principles for the selection of reinsurance counterparties;
- procedures for assessing the creditworthiness and diversification of reinsurance counterparties;
- procedures for assessing the effective risk transfer;
- concentration limits for credit risk exposure to reinsurance counterparties and appropriate systems for monitoring these exposures; and
- liquidity management to deal with any timing mismatch between claims' payments and reinsurance recoveries.

Additional policies and matters to be addressed in policies may also be prescribed.

4.3 The internal control system

4.3.1 IAIS ICP

ICP 8 High level principle

The Supervisor requires an insurer to have, as part of its overall corporate governance framework, effective systems of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters, and internal audit.

Paragraph 8.1.14

The Internal Control System ("ICS") should be designed and operated to assist the Board of Directors and Senior Management in the fulfilment of their respective responsibilities for oversight and management of the company. The ICS provide them with reasonable assurance from a control perspective that the business is being operated consistently with the (a) strategy and risk appetite set by the Board of Directors, (b) agreed business objectives, (c) agreed policies and processes, and (d) laws and regulations.

Paragraph 8.1.21 summary

In addition to other activities that may be appropriate in light of the nature, scale, and complexity of the insurer's business, risks, and obligations, an effective internal controls system should include aspects such as:

- appropriate controls to provide reasonable assurance over the fairness, accuracy, and completeness of the insurer's books, records, and accounts, and over financial consolidation and reporting;
- appropriate controls for other key business processes and policies, including for major business decisions and transactions, critical IT functionalities, access to databases and IT systems by employees, and important legal and regulatory obligations;

- appropriate segregation of duties where necessary, and controls to ensure such segregation is observed.
- up-to-date policies regarding who can sign for or commit the insurer, and for what amounts, with corresponding controls, such as the requirement of double or multiple signatures.;
- controls at the appropriate levels so as to be effective, including at the process or transactional level, at the entity level (whether legal entity or business area level), and, in the case of groups, at the group level;
- a centralised written inventory of key processes and policies insurer-wide, and of the controls in place in respect of such processes and policies;
- training in respect of controls, particularly for employees in positions of high trust or responsibility or carrying out high risk activities;
- processes for regularly checking that the totality of all controls forms a coherent system and that this system (a) works as intended, (b) fits properly within the overall governance structure of the insurer, and (c) provides an element of risk control to complement the risk identification, risk assessment, and risk management activities of the insurer;
- periodic testing and assessments (carried out by objective parties such as internal or external auditor) to determine the adequacy, completeness, and effectiveness of the ICS and its utility to the Board and Senior Management for controlling the operations of the insurer.

Paragraphs 8.1.15 and 8.1.16

At a minimum the ICS should be designed and operated to provide reasonable assurance over (a) the insurer's key business, IT, and financial policies and processes, including in respect of accounting and financial reporting and (b) the related risk management and compliance measures in place. Each individual control of an insurer, as well as all its controls cumulatively, should be designed for effectiveness and operate effectively. Individual controls may be manual (human), automated, or a combination thereof, and may be either general or system or application specific.

The Board of Directors should review and approve the organisational and other measures regarding internal controls. The goal is a coherent system where the controls form a rational insurer-wide framework (from process or transactional level, to entity level, to group level) which can be optimised for maximum effectiveness and efficiency.

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

Paragraph 8.0.2

The systems and functions should be adequate for the nature, scale, and complexity of the insurer's business and risks and should be adapted as the insurer's business and the external environment change.

4.3.2 Solvency II Level I Directive

Article 46 - Internal control

1. Insurance and reinsurance undertakings shall have in place an effective internal control system.

   That system shall at least include administrative and accounting procedures, an internal control framework, and appropriate reporting arrangements at all levels of the undertaking and a compliance function.

4.3.3 Recommendation

Primary legislation:
An insurer must, as part of its governance framework, establish, maintain and operate within an effective internal control system ("ICS"), comprising the totality of strategies, policies, procedures and controls to assist the board of directors and senior management in the fulfilment of their respective responsibilities for oversight and management of the insurer.

The ICS should be appropriate to the nature, scale, and complexity of the insurer's business and risks, and should provide the Board of Directors with reasonable assurance from a control perspective that the business is being operated consistently with the (a) strategy set by the Board of Directors, (b) agreed business objectives, (c) the key business, IT, and financial policies and procedures, including in respect of accounting and financial reporting, and (d) laws and regulations.

The ICS must, at a minimum, provide for;

- appropriate controls to ensure the availability and reliability of financial and non-financial information;
- the development, implementation and regular review of a compliance plan;
- appropriate segregation of duties, and controls to ensure such segregation is observed;
- regular monitoring of all controls to ensure that the totality of controls forms a coherent system and that the ICS functions as intended, fits within the overall governance framework and complements the risk identification, risk assessment, and risk management activities of the insurer.
- regular independent testing and assessments to determine the adequacy, completeness, and effectiveness of the ICS and its usefulness to the Board and Senior Management for controlling the operations of the insurer.

Additional Guidance:

The FSB may include the following criteria in its supervisory assessment of the effectiveness of the internal control system:

- Depending on the nature, scale, and complexity of the insurer's business, risks, and obligations, an effective internal controls system should include aspects such as:
  - appropriate controls for other key business procedures and policies, including for major business decisions and transactions, critical IT functionalities, access to databases and IT systems by employees, and important legal and regulatory obligations;
  - appropriate segregation of duties where necessary, and controls to ensure such segregation is observed.
  - up-to-date policies regarding who can sign for or commit the insurer, and for what amounts, with corresponding controls, such as the requirement of double or multiple signatures.;
  - controls at the appropriate levels so as to be effective, including at the procedure or transactional level, at the entity level (whether legal entity or business area level);
  - a centralised written inventory of key procedures and policies insurer-wide, and of the controls in place in respect of such procedures and policies;
  - training in respect of controls, particularly for employees in positions of high trust or responsibility, or carrying out high risk activities;
  - procedures for regularly checking that the totality of all controls forms a coherent system and that this system works as intended, fits properly within the overall governance structure of the insurer, and provides an element of risk control to complement the risk identification, risk assessment, and risk management activities of the insurer.

5. CONTROL FUNCTIONS

5.1 General requirements for control functions

5.1.1 IAIS ICP

Paragraphs 8.2.3 through 8.2.6 summary

The existence of any control function does not relieve the Board of Directors or Senior Management from their respective governance and related responsibilities.

The control functions (other than internal audit) should be subject to periodic internal or external review by the insurer's internal auditor or an objective external reviewer. The internal audit function should be subject to periodic review by an objective external reviewer.

Paragraphs 8.2.9 through 8.2.14 summary

Each control function should have the necessary authority and independence to be effective in fulfilling its duties and attaining its goals.

The Board of Directors should set or approve the authority and responsibilities of each control function.

The authority and responsibilities of each control function should be set out in writing and made part of or referred to in the governance documentation of the insurer.

Each control function should avoid conflicts of interest. The Board of Directors should ensure that each control function has the authority to communicate on its own initiative with any employee, and has unrestricted access to such information as it needs to carry out its responsibilities.

Paragraph 8.1.20 summary

Reporting on the ICS should cover matters such as:

- the strategy in respect of internal controls;
- the stage of development of the ICS, including the scope that it covers, testing activity, and the performance against annual or periodic ICS goals being pursued;
- information on resources (personnel, budget, etc.) being applied in respect of the ICS;
- an assessment of how the various organisational units or major business areas of the insurer are performing against internal control standards and goals;
- control deficiencies, weaknesses, and failures that have arisen, or that have been identified, and the responses thereto.

Paragraph 8.2.17

The Board of Directors should periodically assess the performance of each control function. This may be done by the full Board, by the Chair of the Board, or by the committee of the Board to which the head of the control function reports or by the Chair of such committee.

Paragraphs 8.2.18 through 8.2.20 summary

Each control function should have the resources necessary to fulfil its responsibilities and achieve the specific goals in its areas of responsibility.

Members of each control function should possess the necessary experience, skills, and knowledge required for the specific position they exercise, and meet any applicable professional qualifications or certifications.

ICP Standard 8.4

An insurer is required to have an effective compliance function capable of assisting the insurer to meet its legal and regulatory obligations, and promote and sustain a corporate culture of compliance and integrity within the insurer.

Paragraphs 8.4.4 and 8.4.3 summary

The compliance function should have access to and report to the Board of Directors on matters such as:

- the strategy of the compliance function;
- the compliance function's operational plan;
- information on its resources;
- an assessment of the key compliance risks the insurer faces and the steps being taken to address them;
- an assessment of how the various parts of the insurer are performing against compliance standards and goals;
- 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;
- 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;
- material fines or other disciplinary actions taken by any regulator or supervisor in respect of the insurer or any employee.

Paragraph 8.4.5 summary

The compliance function should establish, implement, and maintain appropriate mechanisms and activities to:

- promote and sustain an ethical corporate culture that values responsible conduct and compliance with internal and external obligations;
- identify, assess, report on, and address key legal and regulatory obligations and the risks associated therewith;
- ensure the insurer does appropriate monitoring of and has appropriate policies, processes, and controls in respect of key areas of legal, regulatory, and ethical obligation;
- hold regular training on key legal and regulatory obligations, particularly for employees in positions of high trust or responsibility, or who are involved in high risk activities;
- facilitate the confidential reporting by employees of concerns, shortcomings, or potential violations in respect of insurer policies, legal, or regulatory obligations, or ethical considerations;
- address compliance shortcomings and violations;
- conduct regular assessments of the compliance function and the compliance policies and systems, and implement or monitor needed improvements.

ICP Standard 8.3

The supervisor requires the insurer to have an effective risk management function capable of assisting an insurer to timely identify, measure, monitor, manage, and report on its key risks.

Paragraphs 8.3.2 and 8.3.3

The risk management function should have access to and report to the Board of Directors on matters such as:

- the strategy of the risk management function;

- the risk management function's operational plan, including specific annual or other periodic goals being pursued and the performance against such goals;
- information on the risk management function's resources (such as personnel, budget, etc.) including an analysis on the appropriateness of these resources;
- an assessment of risk positions and risk exposures and steps being taken to address them;
- an assessment of changes in the insurer's risk profile;
- where appropriate, an assessment of pre-defined risk limits;
- where appropriate, risk management matters in relation to strategic affairs such as corporate strategy, mergers and acquisitions, and major projects and investments;
- an assessment of risk events and the identification of appropriate remedial actions.

Paragraph 8.3.4

The risk management function should establish, implement and maintain appropriate mechanisms and activities to:

- assist the Board of Directors and Senior Management in carrying out their respective responsibilities, including by providing specialist analysis and performing risk reviews;
- identify the risks the insurer faces;
- assess, aggregate, monitor, and help manage and otherwise address identified risks effectively; this includes assessing the insurer's capacity to absorb risk with due regard to the nature, probability, duration, correlation, and potential severity of risks;
- gain and maintain an aggregated view of the risk profile of the insurer;
- evaluate the internal and external risk environment on an on-going basis in order to identify and assess potential risks as early as possible. This may include looking at risks from different perspective, such as by territory or by line of business;
- consider risks arising from remuneration arrangements and incentive structures;
- conduct regular stress testing and scenario analyses, including in respect of "outliers" or matters with low probability but high potential impact;
- regularly report to Senior Management, 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;
- 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
- conduct regular assessments of the risk management function and the risk management system, and implement or monitor the implementation of any needed improvements.

ICP Standard 8.5

The supervisor requires the insurer to have an effective actuarial function capable of evaluating and providing advice to the insurer regarding, at a minimum, technical provisions, premium and pricing activities, and compliance with the related statutory and regulatory requirements.

Paragraphs 8.5.3 and 8.5.4

The actuarial function should have access to and periodically report to the Board of Directors. The actuarial function should have the authority and obligation to promptly inform the Board of Directors of any circumstance that may have an adverse material effect on the insurer from an actuarial perspective, such as the insurer's solvency reserves or financial condition or if the insurer does not or is unlikely to comply with relevant requirements or legislation.

Written reports on actuarial evaluations should be made to the Board, Senior Management, or other Key Persons in Control Functions or the supervisor as necessary or appropriate or as required by legislation.

Paragraphs 8.5.8 through 8.5.12

Some jurisdictions may require an "appointed actuary," "statutory actuary," or "responsible actuary" (hereinafter referred to as an "Appointed Actuary") to perform certain functions, such as determining or providing advice on an insurer's compliance with regulatory requirements for certifications or statements of actuarial opinion. The tasks and responsibilities of the Appointed Actuary should be clearly defined.

The insurer should be required, at a minimum, to report the Appointed Actuary's appointment to the supervisor.

The Appointed Actuary should not hold positions within or outside of the insurer that may create conflicts of interest or endanger his or her independence. If the Appointed Actuary is not an employee of the insurer, the Board of Directors should determine whether the external actuary has any potential conflicts of interest, such as if his or her firm also provides auditing services to the insurer. If any such conflicts exist, the Board of Directors should subject them to appropriate controls.

If an Appointed Actuary resigns or is removed by an insurer, the insurer should provide notification to the supervisor which includes the reasons why the Appointed Actuary resigned or was replaced. In some jurisdictions, such a notification includes a statement from the insurer regarding whether there were any disagreements with the former Appointed Actuary regarding the content of the actuary's opinion on matters of risk management, required disclosures, scopes, procedures, or data quality, and whether or not such disagreements were resolved to the former Appointed Actuary's satisfaction.

Paragraph 8.5.5 through 8.5.7

The actuarial function should carry out such activities as are needed to evaluate and provide advice to the insurer in respect of technical provisions, premium and pricing activities and compliance with related statutory and regulatory requirements. The actuarial function evaluates and provides advice on things such as:

- the insurer's actuarial and financial risks;
- the insurer's investment policies and the valuation of assets;
- an insurer's solvency position, including a calculation of minimum capital required for regulatory purposes and liability and loss provisions;
- an insurer's prospective solvency position, such as in utilising stress and scenario tests;
- risk assessment and management policies and controls relevant to actuarial matters or the financial condition of the insurer;
- distribution of dividends or other benefits;
- underwriting policies;
- reinsurance arrangements;
- product development and design, including the terms and conditions of insurance contracts.

Where required, the actuarial function may also provide to the supervisor certifications on the adequacy, reasonableness and/or fairness of premiums (or the methodology to determine the same) and certifications or statements of actuarial opinion.

The supervisor should clearly define when such certifications or statements of actuarial opinion need to be filed. When these are required, the supervisor should also clearly define

the required qualifications of those allowed to certify or sign such statements, and what must be included in such an opinion or certification.

ICP Standard 8.6

The supervisor requires the insurer to have an effective internal audit function capable of providing the Board of Directors independent assurance in respect of the insurer's governance, risk management, and internal controls.

Paragraph 8.6.2

The internal audit function should provide independent assurance to the Board of Directors through general and specific audits, reviews, testing, and other techniques in respect of matters such as:

- the overall means by which the insurer preserves its assets, and those of policyholders, and seeks to prevent fraud, misappropriation, or misapplication of such assets;
- the reliability, integrity, and completeness of the accounting, financial reporting, and management information and IT systems;
- the design and operational effectiveness of the insurer's individual controls in respect of the above matters, as well as of the totality of such controls (the internal controls system);
- other matters as may be requested by the Board of Directors, Senior Management, or the supervisor; and
- other matters which the internal audit function determines require review to fulfil its mission, in accordance with its charter, terms of reference, or other documents setting out its authority and responsibilities.

Paragraphs 8.6.3 through 8.6.6

To help ensure objectivity, the internal audit function is fully independent from management and is not involved operationally in the business. The internal audit function's ultimate responsibility is to the Board of Directors, not management. In carrying out its tasks, the internal audit function forms its judgments independently.

The Board of Directors should ensure that the authority granted to the internal audit function includes the authority to:

- access and review any records or information of the insurer which the internal audit function deems necessary to carry out an audit or other review;
- undertake on the internal audit function's initiative a review of any area or any function consistent with its mission;
- require an appropriate management response to an internal audit report, including the development of a suitable remediation, mitigation, or other follow-up plan as needed;
- decline doing an audit or other review, or taking on any other responsibilities requested by management, if the internal audit function believes this is inconsistent with its mission or with the strategy and audit plan approved by the Board of Directors. In any such case, the internal audit function must inform the Board of Directors and seek its guidance.

In its reporting, the internal audit function should cover matters such as:

- the strategy of the function;
- the function's annual or multi-annual operational or audit plan, detailing the proposed areas of audit focus;
- an assessment on the extent of achievement of the goals set out in the operational or audit plan;

- information on its resources (personnel, budget, etc.), including an analysis on the appropriateness of those resources in light of the insurer's size, complexity, risk profile, and legal and regulatory obligations;
- any factors that may be adversely affecting the internal audit function's independence, objectivity, or effectiveness;
- material findings from audits or reviews conducted; and
- the extent of management compliance with agreed upon corrective or risk mitigating measures in response to identified control deficiencies, weaknesses or failures, compliance violations, or other lapses.

Paragraphs 8.6.7 through 8.6.9

- The audit function should carry out such activities as are needed to fulfil the responsibilities described in the foregoing sections. These activities include among others:
  - establishing, implementing and maintaining a risk-based audit plan to examine and evaluate general or specific areas, including on a preventive basis;
  - reviewing and evaluating the adequacy and effectiveness of the insurer's policies and processes and the documentation and controls in respect of these, on a solo and group-wide basis and on an individual subsidiary, business unit, business area, department, or other organisational unit basis;
  - reviewing levels of compliance by employees and organisational units with established policies, processes, and controls, including those involving reporting;
  - evaluating the reliability and integrity of information and the means used to identify, measure, classify, and report such information;
  - ensuring that the identified risks and the agreed actions to address them are accurate and current;
  - evaluating the means of safeguarding insurer and policyholder assets and, as appropriate, verifying the existence of such assets and the required level of segregation in respect of insurer and policyholder assets;
  - monitoring and evaluating governance systems;
  - monitoring and evaluating the effectiveness of the insurer's risk management, compliance, actuary, and other control functions;
  - coordinating with the external auditors and, to the extent requested by the Board of Directors and not inconsistent with applicable law, evaluating the quality of performance of the external auditors;
  - conducting regular assessments of the internal audit function and audit systems and incorporate needed improvements.

  In carrying out the above tasks, the internal audit function should ensure all material areas of risk and obligation of the insurer are subject to appropriate audit or review over a reasonable period of time. Among these areas are those dealing with:

  - market, underwriting, credit, liquidity, operational, and reputational risk;
  - accounting and financial policies and whether the associated records are complete and accurate;
  - extent of compliance by the insurer with applicable law, regulations, rules, and directives from all relevant jurisdictions;
  - intra-group transactions, including intra-group risk transfer and internal pricing;
  - adherence by the insurer to the insurer's compensation policy;
  - 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;

- 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.

Subject to applicable laws on record retention, the internal audit function should keep careful records of all areas and issues reviewed so as to provide evidence of these activities over time.

5.1.2 Solvency II Level I Directive

The compliance function shall include advising the administrative, management or supervisory body on compliance with the laws, regulations and administrative provisions adopted pursuant to this Directive. It shall also include an assessment of the possible impact of any changes in the legal environment on the operations of the undertaking concerned and the identification and assessment of compliance risk.

The compliance function shall be able to communicate on its own initiative with any staff member, and to obtain access to any records necessary to allow it to carry out its responsibilities.

Article 48 - Actuarial function

1. Insurance and reinsurance undertakings shall provide for an effective actuarial function to:
   (a) coordinate the calculation of technical provisions;
   (b) ensure the appropriateness of the methodologies and underlying models used as well as the assumptions made in the calculation of technical provisions;
   (c) assess the sufficiency and quality of the data used in the calculation of technical provisions;
   (d) compare best estimates against experience;
   (e) inform the administrative, management or supervisory body of the reliability and adequacy of the calculation of technical provisions;
   (f) oversee the calculation of technical provisions in the cases set out in Article 82;
   (g) express an opinion on the overall underwriting policy;
   (h) express an opinion on the adequacy of reinsurance arrangements; and
   (i) contribute to the effective implementation of the risk-management system referred to in Article 44, in particular with respect to the risk modelling underlying the calculation of the capital requirements set out in Chapter VI, Sections 4 and 5, and to the assessment referred to in Article 45.
2. The actuarial function shall be carried out by persons who have knowledge of actuarial and financial mathematics, commensurate with the nature, scale and complexity of the risks inherent in the business of the insurance or reinsurance undertaking, and who are able to demonstrate their relevant experience with applicable professional and other standards.

Article 47 - Internal audit

1. Insurance and reinsurance undertakings shall provide for an effective internal audit function. The internal audit function shall include an evaluation of the adequacy and effectiveness of the internal control system and other elements of the system of governance.
2. The internal audit function shall be objective and independent from the operational functions.
3. Any findings and recommendations of the internal audit shall be reported to the administrative, management or supervisory body which shall determine what actions are to be

taken with respect to each of the internal audit findings and recommendations and shall ensure that those actions are carried out.

5.1.3 Solvency II Level II Implementing Advice

EIOPA CP 33

The internal control system shall secure the undertaking's compliance with applicable laws, regulations and administrative provisions and the effectiveness and efficiency of operations in view of its objectives as well as the availability and reliability of financial and non-financial information.
The undertaking shall be required to have in place a suitable control environment, appropriate control activities, effective information and communication procedures and adequate monitoring mechanisms.
The intended compliance activities shall be set out in a compliance plan that ensures that all relevant areas of the insurer are appropriately covered, taking into account their susceptibility to compliance risk.

An insurer shall embed the risk management function in the organisational structure and organise the associated reporting lines in a manner which ensures that the function is objective and free from influence from other functions and from the Board of Directors.
The tasks of the risk management function shall include:
a) Assisting the administrative, management or supervisory body and other management in the effective operation of the risk management system, in particular by performing specialist analysis and performing quality reviews;
b) Monitoring the risk management system;
c) Maintaining an organisation-wide and aggregated view on the risk profile of the undertaking; and
d) Reporting details on risk exposures and advising the administrative, management or supervisory body with regard to risk management matters in relation to strategic affairs like corporate strategy, mergers and acquisitions and major projects and investments; and
e) Identifying and assessing emerging risks.

The actuarial function shall have access to the appropriate resources and information systems that provide all necessary information, relevant for the discharge of its responsibilities.
Informing the administrative, management or supervisory body of the reliability and adequacy of the calculation of the technical provisions is not limited to expressing an opinion on these points, including on the degree of uncertainty about the ultimate outcome and the circumstances that might lead to a significant deviation from the provisions made. The actuarial function must set out how it arrived at its opinion and clearly state and explain any concerns it may have as to the technical provisions being sufficient.
In order to be able to provide its opinions free from influence from other functions and the administrative, management or supervisory body, the actuarial function shall be constituted by persons who have a sufficient level of independency.
In forming and formulating its own actuarial view the actuarial function shall be objective and free from influence of other functions and the administrative, management or supervisory body.

In coordinating the calculation of the technical provisions the actuarial function shall at a minimum:

a) Apply methodologies and procedures to assess the sufficiency of technical provisions ensuring that their calculation is consistent with the underlying principles;
b) Assess the uncertainty associated with the estimates;
c) Produce judgement whenever this is needed, making use of appropriate information and experience of the persons that are in charge of the function;
d) Ensure that problems related to the calculation of technical provisions arising from insufficient data quality are dealt with appropriately and that, where it is impracticable to apply common methods of calculating technical provisions because of insufficient data quality, the most appropriate alternatives to common methods are found, taking into consideration the principle of proportionality;
e) Ensure that homogeneous risk groups for an appropriate assessment of the underlying risks are identified;
f) Consult relevant market information and ensure that it is integrated into the assessment of technical provisions;
g) Compare and justify any material differences among the estimates for different years; and
h) Ensure that an appropriate assessment of options and guarantees embedded in liabilities is provided.

In order to ensure the appropriateness of the underlying methodologies and models used in the calculation of the technical provisions, the actuarial function not only has to assess the general suitability of the methodology or underlying model for the calculation of technical provisions as such, but also has to decide whether they are appropriate for the specific lines of business of the undertaking, for the way the business is managed and for the available data.

While assessing the sufficiency and quality of the data used in the calculation of the technical provisions, the actuarial function shall have regard to the objectivity, reasonability and verifiability of management actions included in the calculation of technical provisions. It shall also assess whether information technology systems used in actuarial procedures sufficiently support these procedures.

The comparison of the best estimates against experience requires the actuarial function to assess whether past best estimates have proved sufficient and to use the insights gained in this assessment to improve the quality of present best estimate calculations.

This analysis shall also include comparisons between observed values and the assumptions used in the calculation of technical provisions in order to produce conclusions on the appropriateness of the data used and the methodologies applied on their estimation.

The actuarial function shall oversee when a case-by-case approach to the calculation of technical provisions shall be followed, that is, when there is not sufficient quality of data to apply a reliable actuarial method. Also, it has to produce judgement to establish assumptions and to safeguard the accuracy of the results.

Regarding the overall underwriting policy, the opinion to be expressed by the actuarial function shall at least include the following issues:
a) Sufficiency of the premiums to cover future losses, notably taking into consideration the underlying risks (including underwriting risks), the impact of expenses directly associated with future claims and of unallocated loss adjustment expenses and the impact of embedded options and guarantees on future liabilities; and
b) Considerations regarding inflation, legal risk, change of mix, anti-selection and adequacy of bonus-malus system(s) implemented in specific line(s) of business.

Regarding the overall reinsurance arrangements, the opinion to be expressed by the actuarial function shall include an opinion on the adequacy of the significant reinsurance arrangements as well as expected cover under stress scenarios in relation to the underwriting policy and the adequacy of the calculation of the technical provisions arising from reinsurance.

The actuarial function shall at least annually produce written reports to be submitted to the administrative, management or supervisory body. The reports shall document the tasks that have been undertaken, clearly state any shortcomings identified and give recommendations as to how the deficiencies could be remedied.

To ensure its independence from the organisational activities audited, the internal audit function shall carry out its assignments with impartiality. The internal audit function shall be able to exercise its assignments on its own initiative in all areas of the undertaking. It shall be free to express its opinions and to disclose its findings and its appraisals to the whole administrative, management or supervisory body.

The internal audit function shall have the complete and unrestricted right to obtain information, which includes the prompt provision of all necessary information, the availability of all essential documentation, and the ability to look into all activities and processes of the insurer relevant for the discharge of its responsibilities, as required in the performance of its tasks, as well as having direct communication with any member of the insurer's staff.

To ensure the effectiveness of the internal audit function, every activity and every unit of the insurer shall fall within its scope. The function shall draw up an audit plan to determine its future auditing actions, taking a risk-based approach in deciding its priorities.
The internal audit function shall at least annually produce a written report on its findings to be submitted to the administrative, management or supervisory body. The report shall cover at least any deficiencies with regard to the efficiency and suitability of the internal control system, as well as major shortcomings with regard to the compliance with internal policies, procedures and processes. It shall include recommendations on how to remedy inadequacies and also specifically address how past points of criticism and past recommendations have been implemented.

5.1.4 Recommendation

Primary legislation:

An insurer must establish and maintain compliance, risk management, actuarial control and internal audit functions ("control functions").

Each control function should have the necessary authority, independence, resources, expertise and access to the board and all relevant employees and information to exercise its authority and perform its responsibilities.

The authority and responsibilities of each control function must be determined and documented in the governance framework of the insurer.

The control functions (other than internal audit) should be subject to regular review by the insurer's internal audit function, or an objective external reviewer.

The internal audit function should be subject to regular review by an objective external reviewer.

The board of directors, taking into consideration the reviews referred to above, must regularly

review the performance of each control function.

The existence of any control function does not relieve the Board of Directors or Senior Management from their respective governance and related responsibilities.

An insurer may, where appropriate in light of the nature, scale and complexity of the insurer's business, risks, and legal and regulatory obligations, outsource a control function. Such an outsourcing arrangement should be considered in the context of the requirements pertaining to outsourcing arrangements.

Secondary legislation

Conflicts of interest should be brought to the attention of the Board of Directors for resolution.

Reporting on the ICS should cover matters such as:

- the strategy in respect of internal controls;
- the stage of development of the ICS, including the scope that it covers, testing activity, and the performance against annual or periodic ICS goals being pursued;
- information on resources (personnel, budget, etc.) being applied in respect of the ICS;
- an assessment of how the various organisational units or major business areas of the insurer are performing against internal control standards and goals;
- control deficiencies, weaknesses, and failures that have arisen, or that have been identified, and the responses thereto.

Secondary legislation: Compliance

As part of their internal control systems insurers are required to have an effective compliance function which ensures that the insurer is able to meet its legal and regulatory obligations, and which promotes and sustains a corporate culture of compliance and integrity.

Depending on the nature, scale, and complexity of its organisation the insurer will appoint a dedicated head of the compliance function. Where an insurer lacks the resources to appoint a dedicated compliance officer, the insurer may apply to the supervisor for any suitably qualified employee of the organisation to carry out this function.

The compliance function should have access to and report to the Board of Directors on matters such as:

- the compliance function strategy;
- the compliance function's operational plan;
- resources available to the compliance function;
- the key compliance risks the insurer faces and the steps being taken to address them;
- how the organisational units or major business areas of the insurer are performing against compliance standards and goals;
- compliance issues involving management or persons in positions of major responsibility within the insurer;
- material compliance violations or concerns involving any other person or unit of the insurer;
- material fines or other disciplinary actions taken by any regulator or supervisor in respect of the insurer or any employee.

The compliance function should have the authority to communicate with any employee on its own initiative, and obtain access to any records required to carry out its responsibilities.

The compliance plan:

- promotes the corporate cultural ethical values that underpin responsible compliance with internal and external obligations;

- identifies all material legal and regulatory obligations and the risks associated therewith;
- documents policies, processes, and controls in respect of all material compliance obligations;
- lays down the regimen for monitoring of all material compliance obligations;
- lays down the regimen for on-going training of relevant staff in respect of compliance obligations; and
- makes provision for confidential reporting by employees of shortcomings or violations of compliance obligations.

The compliance function should regularly report on the insurer's satisfaction of its internal and external compliance obligations.

The compliance function should conduct regular assessments of the compliance function and the compliance policies and systems.

Secondary legislation: Risk Management

The risk management function should have the authority to communicate with any employee on its own initiative, and obtain access to any records required to carry out its responsibilities.

The tasks of the risk management function shall include:

- Assisting the Board of Directors and Senior Management in the effective operation of the risk management system, in particular by performing specialist analysis and performing quality reviews;
- Monitoring the risk management system;
- Maintaining an organisation-wide and aggregated view on the risk profile of the insurer; and
- Reporting details on risk exposures and advising the Board of Directors with regard to risk management matters in relation to strategic affairs like corporate strategy, mergers and acquisitions and major projects and investments; and
- Identifying and assessing emerging risks.

Secondary legislation: Actuarial Control Function

The actuarial control function is responsible for evaluating and providing advice to the insurer regarding, at a minimum, technical provisions, premium and pricing activities, reinsurance arrangements, and compliance with the related statutory and regulatory requirements. Written reports on actuarial evaluations should be made to the Board, Senior Management, or other Key Persons in Control Functions or the supervisor as necessary, or appropriate, or as required by legislation.

Informing the Board of Directors of the reliability and adequacy of the calculation of the technical provisions is not limited to expressing an opinion on these calculations and their degree of uncertainty. The head of the actuarial control function should also set out how they arrived at their opinion and clearly state and explain any concerns they may have as to the technical provisions being sufficient.

The scope of activities for which the head of the actuarial control function bears responsibility will be prescribed in subordinate legislation.

[**Note**: In the interim, to the extent that the roles and responsibilities of the actuarial control function are already being performed by the Statutory Actuary then the provisions relating to those roles and responsibilities of the actuarial control function will fall away.]

[**Note**: This standard will be further developed under the SAM final requirements.]

Secondary legislation: Internal Audit

To ensure that objectivity and independence can be maintained the internal audit function must be able to discharge its duties with impartiality and on its own initiative.

The internal audit function must have unrestricted rights to obtain all information necessary to discharge its responsibilities, to look into all activities and processes of the insurer, and to communicate directly with any member of the insurer's staff.

An insurer must draw up a risk-based internal audit plan to determine future auditing actions.

The internal audit function shall at least annually produce a written report on its findings to be submitted to the Board of Directors. The report must identify material deficiencies of the internal control system, or of compliance with internal policies and procedures, and include recommendations to remedy all identified deficiencies.

Additional Guidance

The actuarial control function should carry out such activities as are needed to evaluate and provide advice to the insurer in respect of technical provisions, premium and pricing activities, reinsurance arrangements, and compliance with related statutory and regulatory requirements. The actuarial function evaluates and provides advice on things such as:

- the insurer's actuarial and financial risks;
- the insurer's investment policies and the valuation of assets;
- the insurer's current solvency position, including a calculation of minimum capital required for regulatory purposes and liability and loss provisions;
- the insurer's prospective solvency position, utilising stress and scenario tests;
- risk assessment and management policies and controls relevant to actuarial matters or the financial condition of the insurer;
- distribution of dividends or other benefits;
- underwriting policies, including opinions as to the sufficiency of premiums to cover future losses, impact of expenses, and impact of embedded options and guarantees on future liabilities;
- reinsurance arrangements, including opinions as to the adequacy of significant reinsurance arrangements, and expected cover under stress scenarios in relation to the underwriting policy;
- product development and design, including the terms and conditions of insurance contracts.

The actuarial control function may also be required to provide the supervisor with certifications on the adequacy, reasonableness and fairness of premiums, or the methodology to determine these, and other certifications or statements of actuarial opinion.

The internal audit function should play a key role in the combined assurance model by providing independent assurance on risk management and internal controls. The move to a combined assurance model is as a result of disparate risk control functions such as risk management, legal, and compliance within an organisation operating in silos with a lack of coordination. The internal audit function, in consultation with the Board of Directors and Senior Management, must define the components of the internal audit framework by which the internal control environment can be measured, according to which the Board of Directors will assess and report on the effectiveness of the system of internal controls.2

In its reporting, the internal audit function should cover matters such as:

[2] King III

- the strategy of the function;
- the function's audit plan, detailing the proposed areas of audit focus;
- an assessment on the extent of achievement of the goals set out in the audit plan;
- information on its resources;
- any factors that may impinge on the internal audit function's independence, objectivity, or effectiveness;
- material findings from audits or reviews conducted; and
- the extent of management compliance with previously agreed upon corrective or risk mitigating measures.

Activities carried out by the internal audit function to be included in additional guidance are as per paragraphs 8.6.7 through 8.6.9 above.

5.2 Heads of control functions

5.2.1 IAIS ICP

Paragraphs 8.2.3 through 8.2.6 summary
The appointment, performance assessment, remuneration, disciplining and dismissal of the head of each control function (other than the head of the internal audit function for which more stringent standards apply) should be done with the approval, or at a minimum with the consultation, of the Board of Directors or the relevant committee thereof.

Paragraphs 8.2.15 and 8.2.16
The Board of Directors should ensure that the head of each control function has the authority and responsibility to report periodically to it or one of its committees. Such reporting should be of sufficient frequency and depth to permit timely and meaningful communication and discussion of material matters.
In addition to periodic reporting, the head of each control function should have the opportunity to communicate directly and periodically meet (without the presence of management) with the chair of the relevant Board committee (e.g. Audit or Risk Committee) and/or with the Chair of the full Board of Directors.

Paragraphs 8.2.18 through 8.2.20 summary
The head of each control function should review regularly with Senior Management the adequacy of the function's resources and request adjustments as necessary.

Paragraphs 8.4.4 and 8.4.3 summary
The head of the compliance function should have the authority and obligation to promptly inform the Board of Directors in the event of (1) any major non-compliance by a member of management or (2) a material non-compliance by the insurer with an external obligation.

Paragraphs 8.3.2 and 8.3.3
The head of the risk management function should have the authority and obligation to promptly inform the Board of Directors of any circumstance that may have an adverse material effect on the risk management system of the insurer.

Paragraphs 8.6.3 through 8.6.6
The head of the internal audit function reports to (a) the Board of Directors (or its Chair, unless the Chair is the CEO, in which case (b) applies); or (b) the Audit Committee (or its Chair).

In its reporting, the internal audit function should cover matters such as:

In addition to periodic reporting, the head of internal audit should be authorised to communicate directly with and meet periodically with the head of the Audit Committee or the Chair of the Board without management present.

5.2.2 Recommendation

Primary legislation

Insurers must appoint a head for each of the control functions.

The appointment, performance assessment, remuneration, disciplining and dismissal of the head of each control function (other than the head of the internal audit function for which more stringent standards apply) should be done with the approval of, or after consultation with, the Board of Directors or the relevant committee thereof.

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

Depending on the nature, scale, and complexity of the insurer's business, risks, and legal and regulatory obligations, an insurer may appoint a person, in full or in part, as the head of more than one control function (other than the head of internal audit). Furthermore, the statutory actuary may be appointed as the head of the actuarial control function, provided that such appointment precludes the statutory actuary from conducting any activities for the insurer which would compromise the independence and oversight requirements of the role of the actuarial control function.

The head of each control function must report regularly to the Board of Directors or one of its committees.

The head of each control function must communicate directly and regularly meet (without the presence of senior management) with the chair of the board of directors or one of its committees (e.g. Audit or Risk Committee).

The head of each of the control functions must, without delay, inform the Board of Directors in the event of any major non-compliance by a member of management, or any material non-compliance by the insurer, and the Registrar, if appropriate steps to rectify the matter are not taken by the board of directors. 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, the head must submit the report without delay to the supervisor.

Secondary legislation:

Where an insurer lacks the resources to appoint a dedicated compliance officer, the insurer may apply to the supervisor for any suitably qualified employee of the organisation to carry out this function.

Where an insurer lacks the resources to appoint a dedicated resource, the insurer may apply to the supervisor for any suitably qualified employee of the organisation to carry out this function. If the Risk Management Function is performed on a group level application may be to be exempted from the requirement to appoint a dedicated head of risk management at the legal entity level if it can be clearly demonstrated and evidenced.

The head of the risk management function has the responsibility to ensure that the insurer is

able to timeously identify, measure, manage, monitor, and report on all material risks.

The head of the risk management function has the authority and responsibility to regularly report to the Board of Directors all material issues regarding the insurer's evolving risk profile, management of the risk function itself, and risk management issues related to strategic affairs as necessary.

Where an insurer lacks the resources to appoint a dedicated head of internal audit, the insurer may apply to the supervisor for any suitable employee of the organisation to carry out this function or for this function to be outsourced.

As part of their internal control systems insurers are required to have an effective internal audit function which provides both an independent assurance role at an entity level, and a control function at an operational level.

To ensure that objectivity and independence can be maintained the internal audit function must be able to discharge its duties with impartiality and on its own initiative.

The internal audit function must have unrestricted rights to obtain all information necessary to discharge its responsibilities, to look into all activities and processes of the insurer, and to communicate directly with any member of the insurer's staff.

The head of the internal audit function must report directly to the Board of Directors or the Audit Committee.

The head of the internal audit function should be authorised to communicate directly with and meet periodically with the head of the Audit Committee or the Chair of the Board without management present.

Additional Guidance

The head of the risk management function is accountable to the Board of Directors in matters pertaining to:

- the strategy of the risk management function;
- the risk management function's operational plan;
- information on the risk management function's resources;
- assessment of material risk positions and risk exposures and the management thereof;
- assessment of the insurer's evolving risk profile;
- assessment of pre-defined risk tolerances;
- risk management matters in relation to strategic affairs such as corporate strategy, mergers and acquisitions, and major projects and investments; and
- assessment of risk events and the identification of appropriate remedial actions.

The head of the risk management function will discharge this responsibility through the following activities:

- establishing an aggregated view of the insurer's current and evolving risk profile;
- evaluating the internal and external risk environment on an on-going basis;
- considering risks arising from remuneration arrangements and incentive structures;
- conducting regular stress testing and scenario analyses;
- reporting to Senior Management, Key Persons in Internal Control Functions, and the Board of Directors on the insurer's risk profile, and detailing all material risk exposures facing the insurer and related mitigation actions;

- documenting and reporting material adverse changes affecting the insurer's risk management system to the Board of Directors; and
- conducting regular assessments of the risk management function and the risk management system.

6. OUTSOURCING

6.1 Requirements pertaining to outsourcing agreements

6.1.1 IAIS ICP

ICP Standard 8.7

The supervisor requires oversight and clear accountability by the insurer for any material function or activity that is outsourced as if these functions or activities were performed internally.

Paragraphs 8.7.1 through 8.7.8

Supervisors should consider issuing rules or guidance in respect of the outsourcing by an insurer of any material function or activity. The general principle is that such outsourcing, whether to external parties or within the same insurance group, should not materially increase risk to the company or materially adversely affect the insurer's ability to manage its risks and meet its legal and regulatory obligations.

The rules or guidance on material outsourcing by the Supervisor should require the Board of an insurer to (a) approve any such outsourcing, (b) before approving, ensure there was an appropriate assessment of the risks of such outsourcing, including in respect of business continuity, and (c) ensure such outsourcing is subject to appropriate controls.

The Board or Senior Management should be required to satisfy themselves as to the expertise and experience of the outsourcing provider.

The supervisor should require insurers which outsource any material function or activity to have in place an appropriate policy for this purpose, setting out the internal review and approvals required and providing guidance on the contractual and other risk issues to consider. This includes considering limits on the overall level of outsourced activities at the insurer and on the number of activities that can be outsourced to the same service provider.

Outsourcing relationships should be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties. When entering into or varying an outsourcing arrangement, an insurer should be required to consider, among other things:

- how the insurer's risk profile will be affected by the outsourcing;
- the service provider's governance, risk management, and internal controls and its ability to comply with applicable laws and with regulations;
- the service providers' service capability and financial viability;
- succession issues to ensure a smooth transition when ending or varying an outsourcing arrangement.

Outsourcing arrangements should be subject to periodic reviews. Periodic reporting thereon should be made to management and the Board.

The Board and Senior Management remain responsible in respect of functions or activities that are outsourced.

Because of the particularly important role that they play in an insurer's governance system, the supervisor should consider issuing additional requirements for the outsourcing by an insurer of any control function or control activity or dedicating more supervisory attention to any such outsourcing.

6.1.2 Solvency II Level I Directive
Article 49 – Outsourcing

1. Member States shall ensure that insurance and reinsurance undertakings remain fully responsible for discharging all of their obligations under this Directive when they outsource functions or any insurance or reinsurance activities.

2. Outsourcing of critical or important operational functions or activities shall not be undertaken in such a way as to lead to any of the following:
(a) materially impairing the quality of the system of governance;

(b) unduly increasing the operational risk;

(c) impairing the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations;

(d) undermining continuous and satisfactory service to policy holders.

3. Insurance and reinsurance undertakings shall, in a timely manner, notify the supervisory authorities prior to the outsourcing of critical or important functions or activities as well as of any subsequent material developments with respect to those functions or activities.

6.1.3 Recommendation

Primary legislation:

An insurer that outsources any function or activity must have an outsourcing policy that includes the matters as may be prescribed.

An insurer may not outsource any aspect of its insurance business that may –

- materially impair the quality of the governance framework of the insurer, or materially adversely affect the insurer's ability to manage its risks and meet its legal and regulatory obligations;
- materially increase risk to the insurer; impair the ability of the Registrar to monitor the insurer's compliance with its regulatory obligations; or
- compromise the fair treatment of or continuous and satisfactory service to policyholders.

An insurer, when outsourcing any function or activity must avoid, and where this is not possible mitigate, any conflicts of interest in respect of the insurance business of an insurer, the interests of policyholders or the business of the other person that performs the outsourcing. Any remuneration paid in respect of outsourcing must –

- be reasonable and commensurate with the actual process, service or activity outsourced;
- not result in any process, service or activity in respect of which commission or a binder fee is payable being remunerated again;
- not be structured in a manner that increases the risk of unfair treatment of policyholders; and

- not be linked to the monetary value of insurance claims repudiated, paid, not paid or partially paid.

The above also applies to any sub-outsourcing.

An insurer must timeously, but no later than one month, prior to the effective date of an outsourcing contract relating to the outsourcing of a control, management or material function, notify the Registrar of –

- the proposed outsourcing;
- the details of the other person to whom the insurer will outsource that function; and
- the key risks associated with the outsourcing and the risk mitigation strategies that will be put in place to address these risks.

A material function includes any function that has the potential, if disrupted, to have a significant impact on the insurer's business operations or ability to manage risks effectively, including risks to the fair treatment of customers.

In determining whether a function is material, an insurer must consider:

- the potential impact of the outsourcing on the policyholders, finances, reputation and the insurer's business operations or a significant part thereof – particularly where the other person may fail to perform over a given period of time;
- The ability of the insurer to maintain appropriate internal controls and meet regulatory requirements; and
- The degree of difficulty and time associated with replacing the other person or performing the function or activity itself.

An insurer must immediately notify the Registrar of any material developments (such as termination, material non-performance and the like) with respect to the outsourcing during the duration of the outsourcing contract.

If an insurer outsources a control function, or part thereof, the board of directors must prior to the outsourcing satisfy itself that the outsourcing will not interfere with the function's independence, objectivity or effectiveness.

The board of directors must regularly review the effectiveness of any arrangement for outsourcing control functions.

Where any control function is outsourced, the remuneration terms under the agreement with the service provider should be consistent with the objectives and approved parameters of the insurer's remuneration policy.

The Registrar on notification of the outsourcing of a control function, may instruct the insurer to outsource the control function to another person, if the Registrar is of the opinion that the person to whom the control function is outsourced is not suitable; or if the outsourcing will detract from an adequate control environment and risk management system, taking into account the nature, scale and complexity of the insurer's business and the risks to which it is exposed.

Senior management and the board of directors remain responsible for the effective functioning of all aspects of the insurer's governance framework and the discharging all of its obligations under this Act regardless of any outsourcing.

This section applies to the outsourcing of a function or activity by an insurer to a reinsurer or by a reinsurer to an insurer, whether under a reinsurance contract or not, but does not apply to the actual insurance provided under a reinsurance contract;

This does not apply to the outsourcing of a function or activity by another person to an insurer; or to rendering services as intermediary as defined in the regulations.

References

Jurisdiction	Title
IAIS	ICP 5 Suitability of Persons (forthcoming)
	ICP 7 Corporate Governance (forthcoming)
	ICP 8 Risk Management and Internal Controls (forthcoming)
	ICP 13 Reinsurance and Other Forms of Risk Transfer (forthcoming)
	ICP 16 Enterprise Risk Management for solvency purposes (forthcoming)
EIOPA	CP 33 System of Governance
	CP 31 Allowance of Financial Risk Mitigation Techniques
	CP 59 Remuneration Issues
OSFI	Corporate Governance Guideline
APRA	LPS 220 Risk Management
	LPG 200 Risk Management
	LPS 310 Audit and Related Matters
	LPS 510 Governance
	LPG 510 Governance
	PPG 511 Remuneration
	LPS 520 Fit and Proper
	LPG 520 Fit and Proper
RSA	King Code of Governance Principles (King III)
	Banks Act
	Companies Act

A. Annexure: Principles Adopted

The corporate governance frameworks that the supervisor has considered include the three lines of defence, segregation of duties, four eyes' principle, and generally accepted risk principles (GARP). Methodologies include the COSO integrated framework and the combined assurance model from King III. The frameworks and methodologies are interrelated as demonstrated below.

Three lines of defence

Best practice monitoring and control of the governance framework may be achieved by allocating responsibility according to the "three lines of defence" principle, with management as the "first line of defence", the control functions (other than internal audit) as the "second line of defence", and internal audit as the "third line of defence". Management is deemed to "own" the controls and the other "lines of defence" are there to help ensure their application and viability.

The first line of defence can be seen as the "doing and recording" with reporting to line management, Executive Committee (EXCO), and through to the CEO who reports to the Board of Directors. The second line of defence consists of the semi –independent control functions, which act as an "internal checking process", usually reporting through the Chief Risk Officer (CRO). Reports to the CRO may include the Actuarial and the Compliance Function. The CRO, if there is one, usually reports to the Risk and / or the Audit Committee, whose chairperson reports through to the Board. The third line of defence is the independent assurance function which is responsible for independent assurance on the governance, risk management, and internal controls. This independent assurance is usually verified by the independent internal control function, being internal audit, and the external control function, being external audit. Reporting is through to the Audit and / or Audit and Risk Committee.

Segregation of duties

An appropriate segregation of responsibilities ensures that the persons responsible for performing tasks are not also responsible for monitoring and controlling the adequacy of this performance.As an example, business should be segregated to ensure that the person having access to the assets (cash, stock, certificates, policies, deposits, and investments etc.) is separate from the person who records the transaction in the books and records. The asset records and the accounting records should be separately kept, and separately and independently reconciled back to each other. The person who has access to the assets should report into a different person, usually "business", from the person who has access to records, usually reporting to a recording or accounting function.

Four-eyes' principle

The "four-eyes' principle" is the principle that prior to implementing any significant decision concerning the insurer at least two persons review any such decision. The principle can best be demonstrated by an example. At the highest level the Chairperson of the Board is responsible for an organisation, with the day-to-day running being delegated to the CEO. The business thus has appropriate segregation of duties with two pairs of eyes responsible for all transactions. An organisation also usually has a semi-independent internal check via the risk management function, and an independent check, being the internal and external audit functions.

COSO integrated framework

A globally accepted integrated governance, risk management, and internal control framework.

Combined assurance model from King III

The principle of the combined assurance model is that within the context of proportionality, risk, and materiality, all risks should be appropriately managed with appropriate levels of governance, risk management, and internal controls so as to ensure that there are no significant gaps and overlaps. The move to a combined assurance model is as a result of disparate risk control functions such as risk management, legal, and compliance within an organisation operating in silos with a lack of coordination.

Figure 1: Corporate Governance Principles

Principles	Combined assurance model (King III)			
Three lines of defence	Line 1		Line 2	Line 3
Four eye principle	Eye 1	Eye 2	Eye 2	Eye 2
Segregation of duties	Access to assets	Access to records	Recon of assets to records	Independent oversight
	Control over assets	Control over records	"Group" Risk oversight Internal check	Internal audit External audit
GARP	Front office	Back office	Middle office	

Figure 2: Three Lines of Defence

	Line 1	Line 2	Line 3
	Doing and recording	Internal check	Independent check
Risk types	EWRM (All risk types)	EWRM (All risk types)	EWRM (All risk types)
Normally include	BU risk functions BU compliance	Group risk functions Group compliance function (1) Appointed Actuary	External Auditors Group Internal Audit Group compliance function (1)
Support functions	BU support functions Including: HR IT Finance etc	Group support functions Including: HR IT Finance etc	
Whistle blowing To whom? On what? Whistle blowing protection		Appointed Actuary Group compliance function Group risk functions	External Auditors Group Internal Audit
Responsible person Responsible committee	CEO EXCO BU risk committees	Chairperson of Risk committee Board Risk committee Management risk committee	Chairperson of Audit committee Board Audit committee
	Board reponsible for everything		

B. Annexure: Constituents of Fit and Proper Requirements

This annexure provides an overview of the IAIS and Solvency II provisions in respect of what constitutes Fitness and Propriety, or 'suitability' in the ICP language.

Section 9 of the Long-term and Short-term Insurance Acts gives the supervisor the power to remove any person who is found not to be Fit and Proper. The supervisor may arrive at this conclusion on the basis of any of a number of criteria used to assess Fitness and Propriety, for which recommendations are provided below.

IAIS ICP

Paragraph 5.0.1
Suitability is an overarching term that means:

- for Board Members, Senior Management, and Key Persons in Control Functions, having the competence and integrity to fulfil their respective roles (also known as being "fit and proper"); and
- for Significant Owners, having the financial soundness and integrity to fulfil their roles.

ICP 5.1 High level principle
Legislation identifies which persons meet suitability requirements.

ICP 5.2 High level principle
The supervisor requires that in order to be suitable, Board Members, Senior Management and Key Persons in Control Functions possess competence and integrity to fulfil their roles. Significant Owners are required to have the financial soundness and integrity necessary to fulfil their roles.

Paragraphs 5.2.1 and 5.2.2 summary
In order to meet suitability requirements a Board Member, a member of the Senior Management and a Key Persons in Control Functions should have the necessary qualities to perform the duties and carry out the responsibilities required in their position.

Competence can be judged from an individual's professional or formal qualifications and knowledge and/or relevant experience within the insurance and financial industries.

When assessing the collective competence of the Board regard should be given to respective duties allocated to individual members.

Paragraph 5.2.5
At a minimum, the necessary qualities of a Significant Owner relate to:

- financial soundness; and
- the integrity demonstrated in personal behaviour and in business conduct.

The presence of any one indicator may, but need not in and of itself, be determinative of a person's suitability. All relevant indicators, such as the pattern of behaviour or a prior refusal of regulatory approval for relevant positions, should be considered in suitability assessment.

Paragraph 5.2.6

Financial soundness is an important element in determining the suitability of Significant Owners. In determining the financial soundness of Significant Owners, besides their source of financing/funding and future access to capital, the supervisor should also consider matters such as, but not limited to whether:

- there are any indicators that they will not be able to meet their debts as they fall due;
- relevant prudential solvency requirements for financial institutions are met;
- they have been subject to any legally valid judgment, debt or order that remains outstanding or has not been satisfied within a reasonable period;
- they have made arrangements with creditors, filed for bankruptcy or been adjudged bankrupt or had assets sequestered; and
- they have been able to provide the supervisor with a satisfactory credit reference.

ICP 5.3 High level principle
The supervisor requires the insurer to demonstrate initially and thereafter, when requested by the supervisor, the suitability of Board Members, Senior Management, Key Persons in Control Functions and Significant Owners. The suitability requirements and the extent of review required depend on the person's position and responsibility.

Paragraph 5.3.4
The supervisor should collect sufficient and appropriate information, or satisfy itself that the insurer has collected such information, in order to assess whether an individual meets suitability requirements. The information to be collected and the supervisor's assessment of such information may differ depending on the position of the person being assessed in relation to the interests to be safeguarded.

For the purpose of collecting information for the assessment, the supervisor should require the submission of a résumé or similar indicating the professional qualifications as well as previous and current positions and experience of the individual and any information necessary to assist in the assessment, such as:

- financial problems or bankruptcy in his/her private capacity;
- financial problems, bankruptcy or winding-up of an entity in which the individual is/was a Significant Owner or a Board Member, a member of the Senior Management or a Key Person in Control Functions;
- civil liability incurred by the individual as a consequence of unpaid debts;
- the suspension, dismissal or disqualification of the individual from a position from acting as a Board Member or a member of the Senior Management of any company or organisation;
- preventive or corrective measures imposed by an authority on entities in which the individual is/was a Significant Owner or a Board Member, a member of the Senior Management or Key Person in Control Functions;
- convictions or pending proceedings against the individual in his/her capacity in respect of civil or criminal cases;
- convictions in criminal cases of an entity in which the individual is/was a Board Member, a member of the Senior Management, a Significant Owner or Key Person in Control Functions;
- outcome of previous assessments of suitability of an individual, or sanctions or disciplinary actions taken against that individual by another supervisor;
- any disciplinary action taken against an individual by a professional organisation in which the individual is or was a member; and
- any other fact or circumstance that could reasonably be considered relevant for the assessment of that individual.

Paragraph 5.3.5

If the Significant Owner that is to be assessed is a legal person or a corporate entity, the supervisor should collect sufficient and appropriate information to assess if it meets the suitability requirements, which should relate to:

- the nature and scope of its business;
- its Significant Owners, where necessary;
- its source of financing/funding and future access to capital;
- the group structure, if applicable, and organisation chart; and
- other relevant factors.

If the Significant Owner is regulated by another supervisor, the suitability assessment done by the latter may be relied upon to the extent that this assessment reasonably meets the requirements of this Standard.

ICP 5.4 High level principle

The supervisor requires insurers to notify the supervisor of any changes in Board Members, Senior Management, Key persons in Control Functions and Significant Owners. They must also notify the supervisor of any circumstances that may materially adversely affect the suitability of its Board Members, Senior Management, Key Persons in Control Functions and Significant Owners.

The supervisor will take appropriate action to rectify the situation when Board Members, Senior Management, Key Persons in Internal Control Functions, or Shareholders Deemed to Exercise Control no longer meet suitability requirements.

Paragraph 5.5.1

The supervisor should have the power to impose various measures in respect of Board Members, Senior Management and Key Persons in Control Functions who do not meet the relevant suitability requirements. Examples of such measures could include the power to:

- request the insurer to provide additional education, coaching or propose the use of external resources in order to achieve the compliance of suitability requirements by an individual in a position as member of the Board, member of the Senior Management or Key Person in Control Functions;
- prevent, delay or revoke appointment of an individual in a position as Board Member, member of the Senior Management or Key Person in Control Functions by the insurer;
- suspend, dismiss or disqualify an individual in a position as member of the Board, member of the Senior Management or Key Person in Control Functions with the insurer, either directly or by ordering the insurer to take these measures;
- order the insurer to appoint a different person for the position in question who does meet the suitability requirements, to reinforce the sound and proper management and control of the insurer;
- take other actions such as impose additional reporting requirements and increase solvency monitoring activities; and
- withdraw or impose conditions on the business licence, especially in the case of a major breach of suitability requirements, taking into account the impact of the breach or the number of members of the Board, Senior Management or Key Persons in Control Functions involved.

<u>Solvency II Level I Directive and Level II Advice</u>

Article 42 of the Level 1 text states:

Insurance and reinsurance undertakings shall ensure that all persons who effectively run the undertaking or have other key functions at all times fulfil the following requirements:

(a) their professional qualifications, knowledge and experience are adequate to enable sound and prudent management (fit); and

(b) they are of good repute and integrity (proper).

Insurance and reinsurance undertakings shall notify the supervisory authority of any changes to the identity of the persons who effectively run the undertaking or are responsible for other key functions, along with all information needed to assess whether any new persons appointed to manage the undertaking are fit and proper.

Insurance and reinsurance undertakings shall notify their supervisory authority if any of the persons referred to in paragraphs 1 and 2 have been replaced because they no longer fulfil the requirements referred to in paragraph 1.

Level II Advice:

Undertakings shall have in place documented policies and procedures to ensure that all persons subject to Article 42 are fit and proper.

Key functions are those considered important or critical in the system of governance and include at least the risk management, the compliance, the internal audit and the actuarial functions. Other functions may be considered key functions according to the nature, scale and complexity of an undertaking's business or the way it is organised.

Undertakings shall notify the supervisory authority of the persons who effectively run the undertaking and which, if any, other key function holders are identified for the undertaking.

When assessing the fitness of a person the supervisory authority shall include an assessment of his/her professional competence. The assessment of professional competence covers the assessment of the competence in terms of management ('management competence') and in the area of the business activities carried out by the (re)insurance undertaking ('technical competence').

Both the assessment of the management and the technical competences of the person at stake shall be based on the person's previous experience, knowledge and professional qualifications and shall demonstrate due skill, care, diligence, and compliance with the relevant standards of the area/sector he/she has worked in.

In addition to the qualifications that enable them to discharge their duties in their specific areas of responsibility, the members of the administrative, management or supervisory body shall, collectively, be able to provide for the sound and prudent management of the undertaking.

When assessing the propriety of a person the supervisory authority shall at least assess his/her reputation. The assessment of the reputation requires the supervisory authority to check whether there are reasons to believe from past conduct that the person may not discharge its duties in line with applicable rules, regulations and guidelines. Such reasons may arise, for instance, from criminal antecedents, financial antecedents or supervisory experience with that person. Insofar as the person's past business conduct is known this could provide reasons to question the person's integrity.

Recommendation

Board Members, Senior Management, Key Persons in Internal Control Functions, and Shareholders Deemed to Exercise Control in terms of the Long-term and Short-term Insurance Acts must be 'fit and proper' to fulfil their respective roles. Fit and proper means that Board Members, Senior Management, and Key Persons in Internal Control Functions must have the competence and integrity to fulfil their respective roles, and that Shareholders Deemed to Exercise Control must have the soundness and integrity to fulfil their roles.

Key Internal Control Functions include at least the Internal Audit Function, Compliance Function, Risk Management Function, and Statutory (Appointed) Actuary.

Fit and proper means that the individual possesses the competence and integrity necessary to perform the duties and carry out the responsibilities required in their position.

Competence can be judged from an individual's professional or formal qualifications and knowledge and/or relevant experience within the insurance and financial industries.

When assessing the collective competence of the Board regard should be given to respective duties allocated to individual members in the context of the effective functioning of the body as a whole.
The necessary qualities of a Shareholder Deemed to Exercise Control include those related both to financial soundness and the integrity demonstrated in personal behaviour and in business conduct.

All relevant indicators should be considered in the fit and proper assessment as the presence of any one indicator need not of itself be determinative of suitability.

In determining the financial soundness of Shareholders Deemed to Exercise Control the supervisor may consider whether:

- there are any indicators that they will not be able to meet their debts as they fall due;
- relevant prudential solvency requirements for financial institutions are met;
- they have been subject to any judgments;
- they have been sequestrated; and
- they have been able to provide the supervisor with a satisfactory credit reference.

The insurer is required to demonstrate initially and thereafter, when requested by the supervisor, the fitness and propriety of Board Members, Senior Management, Key Persons in Internal Control Functions, and Shareholders Deemed to Exercise Control. The suitability requirements and the extent of review required depend on the person's position and responsibility.

Insurers are required to notify the supervisor of any changes in Board Members, Senior Management, Key persons in Internal Control Functions, and Shareholders Deemed to Exercise Control. They must also notify the supervisor of any circumstances that may materially adversely affect the suitability of its Board Members, Senior Management, Key Persons in Internal Control Functions, and Shareholders Deemed to Exercise Control.

The supervisor will impose various measures in respect of Board Members, Senior Management, and Key Persons in Internal Control Functions who do not meet the relevant suitability requirements. Examples of such measures could include:

- requesting the insurer to provide additional education, coaching, or the use of external resources in order to achieve the compliance of suitability requirements by an individual;
- requesting that the appointment of an individual be prevented, delayed, or revoked;
- requesting that an individual be suspended, dismissed, or disqualified;
- requesting the insurer to appoint a different person for the position in question;
- taking other actions such as imposing additional reporting requirements and increase solvency monitoring activities; and
- withdrawing or imposing conditions on the business licence

Additional Guidance

For the purpose of the fit and proper assessment the supervisor requires the submission of a Personal Questionnaire accompanied by a Curriculum Vitae indicating the professional qualifications, as well as previous and current positions and experience of the individual, and any other information necessary to assist in the assessment, such as:

- bankruptcy in his/her private capacity;
- bankruptcy, or winding-up of an entity in which the individual is/was a Shareholder Deemed to Exercise Control or a Board Member, a member of the Senior Management, or a Key Person in Internal Control Function;
- any liability incurred by the individual as a consequence of unpaid debts;
- the suspension, dismissal, or disqualification of the individual from a position from acting as a Board Member, or a member of the Senior Management of any company or organisation;
- preventive or corrective measures imposed by an authority on entities in which the individual is/was a Shareholder Deemed to Exercise Control or a Board Member, a member of the Senior Management, or Key Person in Internal Control Function;
- convictions or pending proceedings against the individual in his/her capacity in respect of civil or criminal cases;
- convictions in criminal cases of an entity in which the individual is/was a Board Member, a member of the Senior Management, a Shareholder Deemed to Exercise Control, or Key Person in Internal Control Function;
- outcome of previous assessments of suitability of an individual, or sanctions or disciplinary actions taken against that individual by another supervisor;
- any disciplinary action taken against an individual by a professional organisation in which the individual is or was a member; and
- any other fact or circumstance that could reasonably be considered relevant for the assessment of that individual.

If the Shareholder Deemed to Exercise Control that is to be assessed is a legal person or a corporate entity, the supervisor will collect sufficient and appropriate information to assess if it meets the fit and proper requirements, which may include:

- the nature and scope of its business;
- its Shareholders Deemed to Exercise Control, where necessary;
- its source of financing/funding and future access to capital;
- the group structure, if applicable, and organisation chart; and any other relevant factors.

C. Annexure: Additional Guidance per APRA and OSFI

D.1 Governance Framework

- Ultimate responsibility for corporate governance rests with the Board of Directors
  (APRA, OSFI)
- Corporate Governance is an important factor in maintaining market confidence; a culture that promotes good governance is of benefit to all stakeholders.
  (APRA, OSFI)
- The supervisor expects insurers to be aware of emerging best practices that are applicable to their institution.
  (OSFI)

D.1.1 Governance Framework Objectives

n/a

D.1.2 Board of Directors: Structure and Governance

- Effective oversight of the business of an insurer by its Board and Senior Management is essential to an efficient supervisory system. It helps protect policyholders, and allows the supervisor to rely on the insurer's internal processes, thereby reducing the amount of supervisory resources needed to meet its mandate. In situations where an insurer is experiencing problems, or where significant corrective action is necessary, the important role of the Board is heightened.
  (OSFI)

a) Structure and Composition

- The Board of a regulated institution must have a minimum of two executive directors at all times;
- A non-executive director is a director who is not a member of management;
- The Board must have a majority of independent directors at all times;
- An independent director is a non-executive director who is free from any business or other association that could materially interfere with the exercise of their independent judgement;
- The chairperson of the Board must be an independent director of the regulated institution;
- A majority of directors present and eligible to vote at all Board meetings must be non-executives;
- The chairperson of the Board cannot have been the Chief Executive Officer (CEO) of the regulated institution at any time during the previous three years or currently.
  (APRA)

- No one structure can be seen as guaranteeing independence. What matters is that a particular structure and the Board's behaviour are effective given the particular circumstances of the insurer. Independence is normally a matter of the Board demonstrating its ability to act independently of management when appropriate and includes such practices as having regular meetings without management present.
  (OSFI)

- The Board of a regulated institution should have in place a formal policy on Board renewal. (APRA)

b) Statutory Audit Committee

- The Statutory Audit Committee should have sufficient powers to enable it to obtain all information necessary for the performance of its functions.
- The Statutory Audit Committee should ensure the adequacy and independence of both the internal and external audit functions.
- The Statutory Audit Committee should establish and maintain policies and procedures for employees of the regulated institution to submit, confidentially, information about accounting, internal control, compliance, audit, and other matters about which the employee has concerns. The Committee should also have a process for ensuring employees are aware of these policies, and for dealing with matters raised by employees under these policies. (APRA)

- The Statutory Audit Committee should have a charter that includes a reference to the fact that the Committee is responsible for the oversight of supervisor statutory reporting requirements, as well as other financial reporting requirements, professional accounting requirements, internal and external audit, and the appointment of the insurer's external auditor.
- Statutory Audit Committee should review the external auditor's engagement at least annually.
- The Statutory Audit Committee should regularly review the internal and external audit plans, ensuring that they cover all material risks and financial reporting requirements of the insurer, and regularly review the findings of audits, ensuring that issues are being managed and rectified in an appropriate and timely manner. It must also review the annual statements of the insurer, evaluate and approve internal control procedures for the insurer, and meet with the independent oversight providers to review their functions and discuss the effectiveness of the insurer's internal controls and reporting practices.
- The members of the Statutory Audit Committee should, at all times, have free and unfettered access to Senior Management, the Internal Auditor, the heads of all risk management functions, the Appointed Actuary, and the External Auditor. (APRA, OSFI)

c) Duties of Individual Board Members

n/a

d) Performance of the Board

n/a

D.1.3 Board of Directors: Roles and Responsibilities

n/a

a) Setting and Overseeing Strategy

n/a

b) Allocation of Oversight and Management Responsibility

- It is the Board's responsibility to satisfy itself that an adequate and effective system of governance, risk management, and internal control is established and maintained, and that Senior Management monitors the effectiveness of all these frameworks. (APRA)

- The Board should ensure that the heads of all the Internal Control Functions, including risk management, compliance, and internal audit, and also the Appointed Actuary, are independent, have the authority to carry out their responsibilities, and have direct access to the Board.
- These functions help the Board validate whether internal controls are working, and whether the institution's operations and results are reliably reported. The supervisor expects Boards a) to satisfy themselves that these functions are in position to operate effectively, and b) to take advantage of the assistance these functions can provide, by familiarising themselves with the work of these functions, reviewing and understanding their reports to the Board, and following up on concerns raised by their findings.
- To assure itself that these functions are in a position to support the Board as expected, the Board in general terms should have processes in place to:
    - recommend to shareholders a suitable nominee for appointment as external auditor;
    - take an active interest in the selection of heads of Internal Control Functions;
    - review the mandates and organisational structures of the internal control functions;
    - require that those who are responsible for fulfilling these functions are independent from the operations under review and free of influences that may affect their ability to perform their responsibilities objectively;
    - require that the internal oversight providers and the external auditor have unrestricted access to the Board, including through periodic meetings without Senior Management present;
    - satisfy itself that those who are responsible for fulfilling these functions have the resources and authority required to perform their duties appropriately;
    - satisfy itself that the remuneration provided to key individuals in each of these functions is consistent with its role and responsibilities;
    - discuss key findings of the reports produced by these functions, understand how material disagreements are dealt with, and follow-up on any concerns raised by these functions; and
    - regularly review the nature of the function being carried out, as well as the adequacy, effectiveness, and independence of those fulfilling these functions.

  (OSFI)

c) Ensuring Fit and Properness

- The Fit and Proper Policy of a regulated institution assists it in prudently managing the risk that responsible persons are not fit and proper. It will form a part of the institution's broader risk management system.
- The responsible persons of a regulated institution are those persons whose conduct is most likely to have a significant impact on its sound and prudent management. These persons generally comprise Board Members, Senior Management, Key Persons in Internal Control Functions, and Shareholders Deemed to Exercise Control.
- Consideration of whether a particular individual is a responsible person takes into account the person's functions and duties and not simply their position title.
- Integrity is demonstrated through evidence regarding character and in personal behaviour and business conduct.
- Under its Fit and Proper Policy an insurer should consider whether the person:
    - has demonstrated a lack of willingness to comply with legal obligations;
    - has breached a fiduciary obligation;
    - has perpetrated or participated in negligent, deceitful, or otherwise discreditable business or professional practices;

  - has been reprimanded, or disqualified, or removed, by a professional or regulatory body in relation to matters relating to the person's honesty, integrity, or business conduct;
  - has seriously or persistently failed to manage personal debts or financial affairs satisfactorily in circumstances where such failure caused loss to others;
  - has been substantially involved in the management of a business or company which has failed, where that failure has been occasioned in part by deficiencies in that management;
  - is of bad repute in any business or financial community or any market; or
  - was the subject of civil or criminal proceedings or enforcement action.
- An annual performance review will typically be the appropriate time for the annual assessment of a responsible person's fitness and propriety. However, if material information adverse to the assessment becomes known to an institution during the year steps should be taken without waiting for the annual performance review.
  (APRA)

d) Design and Implementation of Sound Risk Management and Internal Controls

- Business objectives and strategies are intimately tied to decisions about the particular risks the institution is prepared to take and what means it will use to manage and mitigate these risks.
- The risk management system will differ based on the institution's business mix and risk tolerance.
- Risk management systems and practices will differ, depending on the scope and size of the institution and the nature of its risk exposures. But whatever the particular approach, every institution should have integrated policies that enable the Board and Senior Management to meet their organisation-wide responsibilities.
- Institutions should be in a position to identify all the significant risks they face, assess their potential impact, and have policies in place to manage them effectively.
- The Board has a number of oversight responsibilities with respect to risk management. Effective Board practices include that the Board:
  - have a general understanding of the types of risks to which the financial institution may be exposed and of the techniques used to measure and manage those risks;
  - review and approve the overall risk philosophy and risk tolerance of the institution;
  - review and approve significant policies or changes in policies for accepting, measuring, monitoring, managing, and reporting on the significant risks to which the institution is exposed;
  - require that management have a process for determining the insurer's desired level of capital, taking into account risks assumed, and for ensuring that capital management strategies are in place;
  - require from management timely and accurate reporting on significant risks faced by the institution, the procedures and controls in place to manage these risks, and the overall effectiveness of risk management processes;
  - assure itself that the risk management activities of the institution have sufficient independence, status, and visibility, and are subject to periodic reviews; and
  - include in its reviews of changes in strategies or new business initiatives, a review of required changes in risk management and controls.
- Internal controls should encompass the policies, processes, culture, tasks, and other aspects of an institution that support the achievement of the institution's objectives. They facilitate the efficiency of operations, contribute to effective risk management, assist compliance with applicable laws and regulations, and strengthen capacity to respond appropriately to business opportunities.

- Development and implementation of an adequate and sound system of internal controls is normally the responsibility of Senior Management. The Board of Directors, however, is ultimately responsible for ensuring that such a system is established and maintained. As part of this responsibility, the Board should regularly, at a high level, review the internal controls systems to determine that these work as expected and remain appropriate.
  (OSFI)

e) Setting and Overseeing Duties of Senior Management

- Senior Management has responsibility for day-to-day management of the regulated institution. It is also Senior Management's responsibility to ensure that the Internal Control Functions, including internal audit, compliance, and risk management, and also the Appointed Actuary, have the resources and support to do their work, and the capacity to offer objective opinions and advice to the Board and to Senior Management.
- Senior Management promotes the effectiveness of the Board of Directors by providing the Board with sound advice on the organisational structure, objectives, strategies, plans, and major policies of the financial institution. It sets out and analyses options for the Board, makes and supports recommendations, and provides relevant data and context to enable the Board to reach informed decisions. It facilitates the Board's oversight role by providing relevant, accurate, and timely information to the Board, enabling it to oversee the management and operations of the institution, assess policies, and determine whether the institution is operating in an appropriate control environment. Senior Management also facilitates effective oversight through fostering candid and robust Board discussions.
  (OSFI)

f) Setting and Overseeing Remuneration Policy and Practices

- An insurer must establish and maintain a written Remuneration Policy. The Remuneration Policy must outline the remuneration objectives and the structure of the remuneration arrangements, including, but not limited to, the performance-based remuneration components of the insurer.
- Remuneration arrangements include measures of performance, the mix of forms of remuneration, and the timing of eligibility to receive payments.
- The Board Remuneration Committee, where one exists, should collectively have the requisite competencies to make informed and independent judgments on the suitability of an insurer's remuneration policy.
- The Board should ultimately be satisfied that the overall remuneration policy and practices are consistent with the identified risk appetite and the long-term interests of the insurer and its stakeholders: such as:
  - the components of the overall remuneration policy, particularly the use and balance of fixed and variable components and the provision of other benefits;
  - the performance criteria and their application for the purposes of determining remuneration payments;
  - the individual remuneration of the members of the Board and Senior Management, including the CEO and, the structure of remuneration of major risk-taking staff; and
  - any reports or disclosures on the insurer's remuneration practices provided to the supervisor or the public.
- The Board Remuneration Committee must have a written charter and terms of reference that outline the Committee's roles, responsibilities, and terms of operation. The Remuneration Committee must be provided with the powers necessary to enable it to perform its functions.

- Where these structures are in place, effective coordination between the Board Risk Committee and the Board Remuneration Committee will assist in producing a properly integrated approach to remuneration.
- The Board Remuneration Committee should have the power to engage independent and impartial third-party experts.
- The governance standards require the Board to have in place a Remuneration Policy.
- Insurers with little or no performance-based components of remuneration must nevertheless have a written Remuneration Policy.
- The Remuneration Policy must ensure that the structure of the remuneration of risk and financial control personnel does not compromise the independence of these personnel in carrying out their functions.
- The Remuneration Policy must form part of the insurer's risk management framework.
- The Board Remuneration Committee, where one exists, or the Board of Directors, should periodically review the Remuneration Policy.
- The Remuneration Policy should cover all persons or classes of person whose actions could put the institution's financial soundness at risk:
    - 'responsible persons'
    - risk and financial control personnel
    - persons receiving a significant proportion of performance-based remuneration
- The Remuneration Policy must prohibit persons who receive equity or equity-linked deferred remuneration from hedging their economic exposures to the resultant equity price risk.
- It is possible that senior risk and financial control personnel will also be 'responsible persons', and will therefore be members of both the first and second groups. The Board will need to ensure that the governance requirements in relation to both hedging equity exposures and independence are applied to such persons.
- The Remuneration Policy applies to the insurer as a whole in a proportionate and risk-based way, and contains specific arrangements that take into account the respective roles of the Board of Directors, Internal Control Functions, Senior Management, and Significant Risk-taking Personnel.
- The Remuneration Policy should also cover persons who are not directly employed by the regulated institution.
- The nature of the engagement of such persons is expected to be addressed in the Remuneration Policy as follows:
    - payments to individuals conform to the Remuneration Policy;
    - persons employed by a related body corporate that provides services to the insurer are to be treated as employees of the insurer; and
    - contractual terms concluded with an unrelated body corporate are relevant, rather than the remuneration of individuals employed or engaged by the body corporate.
- The Board Remuneration Committee, where on exists, should have free and unfettered access to risk and financial control personnel and other parties (internal and external) in carrying out its duties;
- Risk measures and judgments play a key role in the risk adjustment of remuneration, as do the accuracy and reliability of measures of profit and loss. Persons whose primary role is risk and financial control are usually relied upon to ensure the integrity of these measures.
- Risk and financial control personnel should be remunerated in a manner that does not compromise their independence in carrying out their risk or financial control functions.
- There should be processes in place for the remuneration of executives who have risk management and financial control responsibilities for the business as a whole.
- For risk management and financial control personnel generally, an appropriate remuneration arrangement may feature a higher proportion of fixed salary to performance-based remuneration than would be the case for personnel with profit centre responsibility.

(APRA)

g) Ensuring Reliable and Transparent Financial Reporting

n/a

h) Communicating Effectively and Transparently

n/a

i) On-going Monitoring and Evaluation of the Governance Framework

n/a

D.2 Risk Management System

n/a

D.2.1 Risk Management Objectives

n/a

D.2.2 Scope and Embedding of the Risk Management System

n/a

D.2.3 Enterprise Risk Management

n/a

D.2.4 Risk Mitigation Techniques

n/a

D.3 Internal Controls System

n/a

D.3.1 Objectives of Internal Controls

- Internal Control Systems (ICS) encompass the policies, procedures, culture, tasks, and other aspects of an institution that support the achievement of the institution's objectives. It facilitates the efficiency of operations, contributes to effective risk management, assists compliance with applicable laws and regulations, and strengthens capacity to respond appropriately to business opportunities.

- The Board should regularly, at a high level, review the system of internal controls to determine that it works as expected and that it remains appropriate. Useful inputs into these reviews include:
  - management reports on the operations and financial condition of the insurer, the performance of risk management and other control systems during the period under review, and any significant non-compliance with controls, the insurer's code of conduct, or with laws and regulations;
  - internal and external audit opinions on the adequacy of controls for the insurer as a whole and for individual business activities, and recommendations for improvements;
  - the ORSA
  - reports by the Appointed Actuary on the value of policy liabilities, on the current and prospective position of the insurer, and on matters that might have a material adverse impact on its financial condition;
  - the audit report on the audited financial statements and all other reports of the external auditor;
  - views, solicited by the Board, of the insurer's external and internal auditors and legal counsel; and
  - the views and observations of the supervisor.

  (OSFI)

D.3.2 General Requirements of Control Functions

n/a

D.3.3 Compliance Function

n/a

D.3.4 Risk Management Function

n/a

D.3.5 Actuarial Control Function

n/a

D.3.6 Internal Audit Function

n/a

D.4 Outsourcing

n/a

D. Annexure: Audit Committee

The current provisions in the Long-term and Short-term Insurance Acts with respect to the Audit Committee (section 23 of the Long-term Act and section 22 of the Short-term Act) are as follows:

(1) The board of directors of a long-term [short-term] insurer shall appoint an audit committee of at least three members of whom at least two shall be independent non-executive directors within the meaning of section 269A(4)(b) and (c) of the Companies Act.

[Subs. (1) substituted by s. 8 of Act 27/2008]

(2) The majority of the members, including the chairperson of the audit committee, shall be persons who are not employees of the long-term short-term] insurer.

(3) The functions of the audit committee, in addition to the functions referred to in section 270A(1) of the Companies Act, are-

[Words preceding para. (a) substituted by s. 8 of Act 27/2008]

(a) to assist the board of directors in its evaluation of the adequacy and efficiency of the internal control systems, accounting practices, information systems and auditing and actuarial valuation processes applied by the long-term [short-term] insurer in the day-to-day management of its business;

(b) to facilitate and promote communication and liaison concerning the matters referred to in paragraph (a) or a related matter between the board of directors and the managing executive, auditor, statutory actuary and internal audit staff of the long-term [short-term] insurer;

(c) to recommend the introduction of measures which the committee believes may enhance the credibility and objectivity of financial statements and reports concerning the business of the long-term [short-term] insurer; and

(d) to advise on a matter referred to the committee by the board of directors.

(3A) The audit committee may appoint an advisor or request any employee of the long-term [short-term] insurer to advise or assist it in the performance of the functions referred to in subsection (3).

[Subs. (3A) inserted by s. 8 of Act 27/2008]

(4) If the appointment or composition of an audit committee is, in a particular case, inappropriate or impractical or would serve no useful purpose, the Registrar may, subject to such conditions as the Registrar may determine, exempt the long-term [short-term] insurer concerned from the requirements of subsection (1).

[Subs. (4) substituted by s. 8 of Act 27/2008]

E. Annexure: Statutory Actuary

The current provisions in the Long-term and Short-term Insurance Acts with respect to the Statutory Actuary (section 20 of the Long-term Act and 19A of the Short-term Act) are as follows:

(1) A long-term [short-term] insurer shall from time to time appoint, and at all times have, an actuary.

(2) A long-term [short-term] insurer may appoint an alternate to act in the place of its statutory actuary during his or her absence for any reason.

(3) No person other than a natural person who is permanently resident in the Republic is a Fellow of the Actuarial Society of South Africa and has, as an actuary, appropriate practical experience relating to long-term [short-term] insurance business, shall be appointed as a statutory actuary or his or her alternate.

(4) No appointment of a statutory actuary or his or her alternate shall take effect unless it has been approved by the Registrar.

(5) The statutory actuary of a long-term [short-term] insurer shall -

(a) submit to the Registrar, if his or her appointment is for any reason terminated, a statement of what he or she believes to be the reasons for that termination; and

(b)

(i) without delay, report in writing to the board of directors of the long-term [short-term]insurer any matter relating to the business of the long-term [short-term] insurer of which he or she becomes aware in the performance of his or her functions as statutory actuary and which, in his or her opinion, constitutes a contravention of section 29(1) or any other section of this Act relating to the duties of the statutory actuary, or in future may prejudice the long-term insurer's ability to comply with section 29(1) or any other section of this Act relating to the duties of the statutory actuary, which report must give a description of the matter and must include such other particulars as the statutory actuary considers appropriate: Provided that the report must be submitted without delay also to the Registrar where, in the opinion of the statutory actuary, the matter-

(aa) materially prejudices the insurer's ability to comply with any of these sections;

(bb) does not materially prejudice the insurer's ability to comply with these sections, but the statutory actuary is of the opinion that immediate remedial action must be taken by the long-term [short-term] insurer; and

(ii) if steps to rectify the matter are not taken by the board of directors of the long-term [short-term] insurer to the satisfaction of the statutory actuary within 30 days after the date of the report, without delay inform the Registrar.

[Para. (b) substituted by s. 7 of Act 27/2008]

(6)

(a) The furnishing, in good faith, by a statutory actuary of a report or information in terms of subsection (5) shall not be deemed to constitute a contravention of a provision of a law or a breach of a provision of a code of professional conduct to which he or she is subject.

(b) The failure, in good faith, by a statutory actuary to furnish a report or information in terms of this section shall not confer upon any person a right of action against the statutory actuary which, but for that failure, that person would not have had.

(7) In addition to duties assigned to the statutory actuary by any other law or a code of professional practice, the statutory actuary shall -

(a) in relation to a statement forming part of the returns in respect of which he or she is required to do so in terms of section 36, examine that statement and satisfy himself or herself that it is properly drawn up so as to comply with the requirements of this Act and attest or, as the case may be, express an opinion in connection with that statement; and

(b) carry out the other duties provided in this Act or prescribed by the Minister.

(8) A statutory actuary shall -

(a) have the right of access at all times to the accounting records and other books and documents of the long-term [short-term] insurer and be entitled to require from the directors or officers of that insurer the information and explanations he or she deems necessary for the carrying out of his or her duties;

(b) be entitled to -

(i) attend and speak at a general meeting of the long-term [short-term] insurer; and

(ii) receive the notices and other communications relating to a general meeting which a member of that long-term [short-term] insurer is entitled to receive;

[Para. (b) substituted by s. 7 of Act 27/2008]

(c)

(i) attend and be entitled to speak at any meeting of the board of directors of the long-term [short-term] insurer on the business of the meeting which concerns the duties conferred on or assigned to him or her as statutory actuary by or under this Act and by any other law or code of professional practice; and

(ii) receive the notices and other communications relating to any meeting referred to in subparagraph (i) which a member of the board of directors is entitled to receive.

[Para. (c) substituted by s. 7 of Act 27/2008]

The current provisions in the Long-term and Short-term Insurance Acts with respect to the appointment of a Statutory Actuary or Auditor (section 21 of the Long-term Act and section 20 of the Short-term Act) are as follows:

(1) If a long-term [short-term] insurer for any reason fails to appoint -

(a) an auditor in terms of section 19(1), the Registrar may, notwithstanding sections 269(4) and 271(1) of the Companies Act, but subject to section 19 of this Act, appoint an auditor for that long-term [short-term] insurer;

(b) an actuary in terms of section 20(1), the Registrar may, subject to section 20, appoint an actuary for that long-term [short-term] insurer.

(2) A person or firm appointed under subsection (1) as auditor or actuary of a long-term [short-term] insurer shall be deemed to have been appointed by the long-term [short-term] insurer in accordance with this Act.

F. Annexure: Enterprise Risk Management (ERM)

Given that the IAIS' forthcoming standards devote a chapter to Enterprise Risk Management (ERM), an extract of the high level principles thereof in this annexure. It must be noted that ICP 16 deals with risk management (ERM) explicitly for solvency purposes, and also that these provisions are not relevant for the interim measures.

IAIS ICP

Paragraphs 16.0.3 through 16.0.8 summary
Several different terms are commonly used to describe the process of identifying, assessing, measuring, monitoring, controlling and mitigating risks. This ICP uses the generic term enterprise risk management (ERM) in describing these activities in respect of the insurance enterprise as a whole.

ERM involves the self-assessment of all reasonably foreseeable and relevant material risks that an insurer faces and their interrelationships. Hence ERM enables decisions regarding risk management and capital allocation to be co-ordinated for maximum financial efficiency and the adequate protection of policyholders.

Adopting a total balance sheet approach to underpin ERM allows the impact of the totality of material risks to be recognised on an economic basis through the provision of a common measurement basis across all risks (e.g. same methodology, time horizon, risk measure, level of confidence, etc.) and enhance strategic decision-making, for example capital allocation and pricing. A total balance sheet approach reflects the interdependence between assets, liabilities, capital requirements, and capital resources, and identifies a capital allocation, where needed, to protect the insurer and its policyholders and to optimise returns to the insurer on its capital.

ERM provides a link between the on-going operational management of risk and longer-term business goals and strategies. Appropriate risk management policies should be set by each insurer according to the nature, scale, and complexity of its business and the risks it bears.

a) Risk Identification and Measurement

IAIS ICP

ICP 16.1 High level principle
The supervisor requires the insurer's ERM Framework to provide for the identification and quantification of risk under a sufficiently wide range of outcomes, using techniques which are appropriate to the nature, scale, and complexity of the risks the insurer bears, and adequate for risk and capital management and for solvency purposes.

b) Documentation

IAIS ICP

ICP 16.2 High level principle
The supervisor requires the insurer's measurement of risk should be supported by accurate documentation providing appropriately detailed descriptions and explanations of the risks covered, the measurement approaches used, and the key assumptions made.

c) Risk Management Policy

IAIS ICP

ICP 16.4, 16.5, 16.6, and 16.7 High level principles
The insurer's Risk Management Policy should outline how all relevant and material categories of risk are managed, both in the insurer's business strategy and its day-to-day operations.

The insurer's Risk Management Policy should describe the relationship between the insurer's tolerance limits, regulatory capital requirements, economic capital, and the processes and methods for monitoring risk.

The insurer's Risk Management Policy should include an explicit asset-liability management (ALM) policy which clearly specifies the nature, role, and extent of ALM activities, and their relationship with product development, pricing functions, and investment management.
The insurer's Risk Management Policy should incorporate an explicit Investment Policy which:

- specifies the nature, role and extent of the insurer's investment activities.
- establishes 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.

The insurer's Risk Management Policy should include explicit policies in relation to underwriting risk.

d) Risk Tolerance Statement

IAIS ICP

ICP 16.8 High level principle
The supervisor requires the insurer to:

- establish and maintain a risk tolerance statement which sets out its overall quantitative and qualitative risk tolerance levels and defines risk tolerance limits which take into account all relevant and material categories of risk and the relationships between them;
- make use of its risk tolerance levels in its business strategy; and

- embed its defined risk tolerance limits in its day-to-day operations via its risk management policies and procedures.

e) Risk Responsiveness and Feedback Loop

IAIS ICP

ICP 16.9 and 16.10 High level principle
The insurer's ERM Framework should be responsive to changes in its risk profile.
The insurer's ERM framework should incorporate a feedback loop, based on appropriate and good quality information, management processes, and objective assessment, which enables it to take the necessary action in a timely manner in response to changes in its risk profile.

f) Own Risk and Solvency Assessment (ORSA)

IAIS ICP

ICP 16.11, 16.12, 16.13, and 16.14 High level principles
The insurer should perform its Own Risk and Solvency Assessment (ORSA) regularly to assess the adequacy of its risk management, and current and likely future, solvency position.
The Board of Directors is ultimately responsible for conducting the ORSA and assuring its effectiveness by means of independent review.
The ORSA should encompass all reasonably foreseeable and relevant material risks including, as a minimum, underwriting, credit, market, operational, and liquidity risks, and additional risks arising due to membership of a group. The assessment is required to identify the relationship between risk management and the level and quality of financial resources needed and available.
The insurer should be able to:

- determine, as part of its ORSA, the overall financial resources it needs to manage its business given its own risk tolerance and business plans, and to demonstrate that supervisory requirements are met;
- base its risk management actions on consideration of its economic capital, regulatory capital requirements, and financial resources, including its ORSA;
- assess the quality and adequacy of its capital resources to meet regulatory capital requirements and any additional capital needs.
- analyse its ability to continue in business, and the risk management and financial resources required to do so over a longer time horizon than typically used to determine regulatory capital requirements.
- address a combination of quantitative and qualitative elements in the medium and longer term business strategy of the insurer, and include projections of its future financial position and analysis of its ability to meet future regulatory capital requirements.

g) Role of Supervision

IAIS ICP

ICP 16.16 High level principle

The supervisor undertakes reviews of an insurer's risk management processes and its financial condition, including the ORSA. Where necessary, the supervisor requires strengthening of the insurer’s risk management, solvency assessment and capital management processes.

G. Annexure: Board Composition: King III Principles and Companies Act Review

The King Code of Governance Principles (King III) makes the following recommendations in respect of the Chairman of the Board and the composition of the Board of Directors.

Principle 2.16: The board should elect a chairman of the board who is an independent non-executive director. The CEO of the company should not also fulfil the role of chairman of the board.

37. The board should elect a chairman who can provide the direction necessary for an effective board. The chairman should be appointed by the board every year after carefully monitoring his independence and factors that may impair his independence as discussed in this Chapter. Any factor affecting the independence of the chairman should be weighed against the positive factor of continuity of the chairman.

38. The chairman of the board should be independent and free of conflicts of interest at appointment, failing which, the board should appoint a lead independent non-executive director (LID) (refer to Annex 2.1). In situations where the independence of the chairman is questionable or impaired, a LID should be appointed for as long as the situation exists.

39. If the board appoints a chairman who is a non-executive director but is not independent or is an executive director, this should be disclosed in the integrated report, together with the reasons and justifications for the appointment.

40. The chairman‘s role and functions should be formalised. These will be influenced by matters such as the lifecycle or circumstances of the company, the complexity of the company‘s operations, the qualities of the CEO and the management team, as well as the skills and experience of each board member. Core functions performed by the chairman should include the following:

    40.1 setting the ethical tone for the board and the company;
    40.2 providing overall leadership to the board without limiting the principle of collective responsibility for board decisions, while at the same time being aware of the individual duties of board members;
    40.3 identifying and participating in selecting board members (via a nomination committee), and overseeing a formal succession plan for the board, CEO and certain senior management appointments such as the chief financial officer (CFO);
    40.4 formulating (with the CEO and company secretary) the yearly work plan for the board against agreed objectives, and playing an active part in setting the agenda for board meetings;
    40.5 presiding over board meetings and ensuring that time in meetings is used productively. The chairman should encourage collegiality among board members without inhibiting candid debate and creative tension among board members;
    40.6 managing conflicts of interest. It is not sufficient merely to table a register of interests. All internal and external legal requirements must be met. The chairman must ask affected directors to recuse themselves from discussions and decisions in which they have a conflict, unless they are requested to provide specific input, in which event they should not be party to the decision. See section 75 of the Act;
    40.7 acting as the link between the board and management and particularly between the board and the CEO;

40.8 being collegial with board members and management while at the same time maintaining an arm‘s length relationship;
40.9 ensuring that directors play a full and constructive role in the affairs of the company and taking a lead role in the process for removing non-performing or unsuitable directors from the board;
40.10 ensuring that complete, timely, relevant, accurate, honest and accessible information is placed before the board to enable directors to reach an informed decision;
40.11 monitoring how the board works together and how individual directors perform and interact at meetings. The chairman should meet with individual directors once a year about evaluating their performance. The chairman should know board members‘ strengths and weaknesses;
40.12 mentoring to develop skill and enhance directors‘ confidence (especially those new to the role) and encouraging them to speak up and make an active contribution at meetings. The mentoring role is encouraged to maximise the potential of the board;
40.13 ensuring that all directors are appropriately made aware of their responsibilities through a tailored induction programme, and ensuring that a formal programme of continuing professional education is adopted at board level;
40.14 ensuring that good relations are maintained with the company‘s major shareholders and its strategic stakeholders, and presiding over shareholders‘ meetings;
40.15 building and maintaining stakeholders‘ trust and confidence in the company;
40.16 upholding rigorous standards of preparation for meetings by for example, meeting with the CEO before meetings and studying of the meeting information packs distributed; and
40.17 ensuring that decisions by the board are executed.

41. The chairman‘s ability to add value to the company, and the chairman‘s actual performance against criteria developed from his formalised role and functions, should form part of a yearly evaluation by the board.

42. The retired CEO should not become the chairman of the board until three complete years have passed since the end of the CEO‘s tenure as an executive director. After this period, the CEO may be considered for appointment as a non-executive chairman, after an assessment of his independence.

43. The chairman, together with the board, should carefully consider the number of outside chairmanships that he holds. The relative size and complexity of the companies in question should be taken into account. In this regard, chairmen of boards and board committees should apply their minds, in an intellectually honest manner, and be satisfied that they have the ability and capacity to discharge their duties.

44. The chairman should meet with the CEO or the CFO or the company secretary or all three before a board meeting to discuss important issues and agree on the agenda.

45. With regard to the chairman serving on other committees:

45.1 the chairman should not be a member of the audit committee;
45.2 the chairman should not chair the remuneration committee, but may be a member of it;
45.3 the chairman should be a member of the nomination committee and may also be its chairman; and
45.4 the chairman should not chair the risk committee but may be a member of it.

46. There should be a succession plan for the position of the chairman.

Principle 2.18: The board should comprise a balance of power, with a majority of non-executive directors. The majority of non-executive directors should be independent

62. Given the positive interaction and diversity of views that occur between individuals of different skills, experience and backgrounds, the unitary board structure with executive directors (refer to Annex 2.2) and non-executive directors (refer to Annex 2.3) interacting in a working group remains appropriate for South African companies. The unitary system has been well established in South Africa.

63. The board should ensure that there is an appropriate balance of power and authority on the board. No one individual or block of individuals should be able to dominate the board‘s decision-making. 64.

The board should comprise a majority of non-executive directors. The majority of non-executive directors should be independent as this reduces the possibility of conflicts of interest and promotes objectivity.

65. Independent non-executive directors should be independent in fact and in the perception of a reasonably informed outsider. Although independence of mind is essential, perceptions of independence are important.

66. An independent director should be independent in character and judgement and there should be no relationships or circumstances which are likely to affect, or could appear to affect this independence. Independence is the absence of undue influence and bias which can be affected by the intensity of the relationship between the director and the company rather than any particular fact such as length of service or age.

67. An independent non-executive director is a non-executive director who:

67.1 is not a representative of a shareholder who has the ability to control or significantly influence management or the board;
67.2 does not have a direct or indirect interest in the company (including any parent or subsidiary in a consolidated group with the company) which exceeds 5% of the group‘s total number of shares in issue.
67.3 does not have a direct or indirect interest in the company which is less than 5% of the group‘s total number of shares in issue, but is material to his personal wealth;
67.4 has not been employed by the company or the group of which it currently forms part in any executive capacity, or appointed as the designated auditor or partner in the group‘s external audit firm, or senior legal adviser for the preceding three financial years;
67.5 is not a member of the immediate family of an individual who is, or has during the preceding three financial years, been employed by the company or the group in an executive capacity;
67.6 is not a professional adviser to the company or the group, other than as a director;
67.7 is free from any business or other relationship (contractual or statutory) which could be seen by an objective outsider to interfere materially with the individual‘s capacity to act in an independent manner, such as being a director of a material customer of or supplier to the company; or
67.8 does not receive remuneration contingent upon the performance of the company.

68. While the availability or otherwise of sufficiently experienced directors will be a challenge, shareholders should strive to constitute their boards with a majority of independent directors among their non-executive directors.

69. A balance should be sought between continuity in board membership, subject to performance and eligibility for re-election as well as considerations of independence and the sourcing of new ideas through introducing new board members.

70. When determining the number of directors to serve on the board, the collective knowledge, skills, experience and resources required for conducting the business of the board should be considered. Factors determining the number of directors to be appointed are:

    70.1 evolving circumstances, the needs of the company and the nature of its business;
    70.2 the need to achieve an appropriate mix of executive and independent non-executive directors;
    70.3 the need to have sufficient directors to structure board committees appropriately;
    70.4 potential difficulties of raising a quorum with a small board;
    70.5 regulatory requirements; and
    70.6 the skills and knowledge needed to make business judgement calls on behalf of the company.

71. Every board should consider whether its size, diversity and demographics make it effective. Diversity applies to academic qualifications, technical expertise, relevant industry knowledge, experience, nationality, age, race and gender.

72. Directors should be individuals of integrity and courage, and have the relevant knowledge, skills and experience to bring judgement to bear on the business of the company. In situations where directors may lack experience, detailed induction and formal mentoring and support programmes should be implemented.

73. As a minimum, two executive directors should be appointed to the board, being the chief executive officer (CEO) and the director responsible for the finance function. This will ensure that there is more than one point of contact between the board and the management. From June 2009, listed companies must appoint a financial director to the board.

74. A programme ensuring a staggered rotation of non-executive directors should be put in place by the board to the extent that it is not already regulated by the company‘s memorandum of incorporation or relevant regulation. Rotation of board members should be structured so as to retain valuable skills, maintain continuity of knowledge and experience and introduce people with new ideas and expertise.

75. At least one-third of non-executive directors should retire by rotation yearly, usually at the company‘s AGM or other general meetings, unless otherwise prescribed through any applicable legislation. These retiring board members may be re-elected, provided they are eligible. The board, through the nomination committee, should recommend eligibility, considering past performance, contribution and the objectivity of business judgement calls.

76. Every year, non-executive directors classified as ‘independent‘ should undergo an evaluation of their independence by the chairman and the board. If the chairman is not independent, the process should be led by the LID. Independence should be assessed by weighing all relevant factors that may impair independence. The classification of directors in the integrated report, as independent or otherwise, should be done on the basis of this assessment

77. Any term beyond nine years (e.g. three three-year terms) for an independent non-executive director should be subject to a particularly rigorous review by the board, of not only the performance of the director, but also the factors that may impair his independence at that time. The review should also take into account the need for refreshing the board.

78. Independent non-executive directors may serve longer than nine years if, after an independence assessment by the board, there are no relationships or circumstances likely to affect, or appearing to affect, the director‘s judgement. The assessment should show that the independent director‘s independence of character and judgment is not in any way affected or impaired by the length of service. A statement to this effect should be included in the integrated report.

79. The memorandum of incorporation of the company should allow the board to remove any director from the board, including executive directors. Shareholder approval is not necessary for these decisions, provided this is included in the memorandum of incorporation.

Companies Act, 1971	Companies Act, 2008	Banks Act, 1990	King III	APRA	Proposal
COMPOSITION OF BOARD					
Every public company shall have at least two directors	(2) The board of a company must comprise, in the case of a public company, at least three directors	(3) Notwithstanding anything to the contrary in any law or the common law or in any agreement contained, not more than 49 per cent, rounded off to the next lower integral number, of the directors of— (*a*) a bank shall be employees of that bank or of any of its subsidiaries, or of such bank's controlling company, or of any of such controlling company's subsidiaries;	The board should elect a chairman of the board who is an independent non-executive director. The CEO of the company should not also fulfil the role of chairman of the board The board should comprise a balance of power, with a majority of non-executive directors. The majority of non-executive directors should be independent	The Board of a regulated institution must have a minimum of two executive directors at all times; The Board must have a majority of independent directors at all times; The chairperson of the Board must be an independent director of the regulated institution; A majority of directors present and eligible to vote at all Board meetings must be non-executives; The chairperson of the Board cannot have been the Chief Executive Officer (CEO) of the regulated institution at any time during the previous three years or currently.	(i) the board of directors of a long-term insurer must at all times consist of a majority of independent directors and at least two executive directors; and (ii) the chairperson of the board of directors of a long-term insurer must at all times be an independent director

Companies Act, 1971	Companies Act, 2008	Banks Act, 1990	King III	APRA	Proposal
DEFINITION OF INDEPENDENT					
In the context of audit committees A director is a non-executive director of a company if the director— (i) is not involved in the day to day management of the business and has not in the past three financial years been a full-time salaried employee of the company or its group; (ii) is not a member of the immediate family of an individual mentioned in subparagraph (i); A director acts independently if that director—	*In the context of audit committees* (4) Each member of an audit committee of a company must— (*a*) be a director of the company, who satisfies any applicable requirements prescribed in terms of subsection (5); (*b*) not be— (i) involved in the day-to-day management of the company's business or have been so involved at any time during the previous financial year; (ii) a prescribed officer, or full-time employee, of the company or another	*In the context of audit committees* (3) (*a*) All of the members of the audit committee of a bank shall be persons who are not employees of the bank nor of any of its subsidiaries, its controlling company or any subsidiary of its controlling company: Provided that the chairperson of the board of directors of the bank or the controlling company shall not be appointed as a member of the audit committee. (*b*) All of the members of the audit committee of a controlling company shall be persons who are not employees of	Independence is the absence of undue influence and bias which can be affected by the intensity of the relationship between the director and the company	A non-executive director is a director who is not a member of management; An independent director is a non-executive director who is free from any business or other association that could materially interfere with the exercise of their independent judgement;	(b) For purposes of paragraph (a), an independent director means a non-executive director that – (i) is not involved in the day-to-day management of the business of the long-term insurer and has not in the past three financial years been an employee of the long-term insurer or any of its related persons; (ii) is not a member of the immediate family of an individual mentioned in subparagraph (i); or (iii) is not related to the company or any shareholder, supplier, customer or other

Companies Act, 1971	Companies Act, 2008	Banks Act, 1990	King III	APRA	Proposal
(i) expresses opinions, exercises judgment and makes decisions impartially; (ii) is not related to the company or to any shareholder, supplier, customer or other director of the company in a way that would lead a reasonable and informed third party to conclude that the integrity, impartiality or objectivity of that director is compromised by that relationship	related or inter-related company, or have been such an officer or employee at any time during the previous three financial years; or (iii) a material supplier or customer of the company, 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 (*c*) not be related to any person who falls within any of the criteria set out in paragraph (*b*).	the controlling company nor of any of its subsidiaries, the bank in respect of which it is the controlling company or any subsidiary of that bank: Provided that the chairperson of the board of directors of the controlling company or the bank in respect of which it is the controlling company shall not be appointed as a member of the audit committee. (4) The Registrar may upon written application exempt the board of directors of a bank from the duty to appoint an audit committee in respect of a bank if the Registrar is satisfied that the audit committee appointed in respect of the relevant controlling company, in addition to its responsibilities in respect of that			director of the company in a way that would lead a reasonable and informed third party to conclude that the integrity, impartiality or objectivity of that director is compromised.

Companies Act, 1971	Companies Act, 2008	Banks Act, 1990	King III	APRA	Proposal
		controlling company, is able to also adequately assume the responsibilities of an audit committee in respect of that bank			