

ICP 5 Suitability of Persons

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.

Introductory Guidance

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.

5.1 Legislation identifies which persons meet suitability requirements.

5.1.1 At a minimum, the legislation should include Board Members, Senior Management, Key Persons in Control Functions and Significant Owners. Suitability requirements may extend to other individuals to account for the duties and responsibilities of such individuals that may differ depending on the jurisdiction and the legal form and governance structure of the insurer. Some jurisdictions may impose these requirements and apply these tests also to other individuals including financial controllers and treasurers.

5.2 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.

Suitability requirements for Board Members, Senior Management and Key Persons in Control Functions

5.2.1 In order to meet suitability requirements, a Board Member, a member of the Senior Management and a Key Person in Control Functions should have the necessary qualities that will allow that individual to perform the duties and carry out the responsibilities required in his/her position in the insurer.

5.2.2 Competence can generally be judged from the level of an individual’s professional or formal qualifications and knowledge

and/or relevant experience within the insurance and financial industries or other businesses. Competence also includes having the appropriate level of commitment to perform the role. (Please also refer to ICP7:Corporate Governance)

When assessing the competence of the members of collective organs of an insurer (e.g. the Board), regard should be given to respective duties allocated to individual members to ensure appropriate diversity of qualities and to the effective functioning of the collective organ as a whole.

5.2.3 Integrity is demonstrated through evidence regarding character and in personal behaviour and business conduct. The conduct and actions of the individual who is subject to the suitability requirements should be such that his/her integrity is to the satisfaction of the supervisor.

5.2.4 Indicators for an individual's assessment in terms of suitability include criminal, financial, supervisory and other aspects. 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, should be considered in suitability assessment. Examples of indicators could be as follows:

- Criminal indicators: The individual should not have a record or evidence of previous conduct and activities where he/she has been convicted of a criminal offence such as under any legislation designed to protect members of the public from financial loss, e.g. dishonesty, or misappropriation of assets, embezzlement and other fraud or other criminal offences (including anti-money laundering and the combating of the financing of terrorism (AML/CFT) matters). In assessing this indicator, the supervisor should recognise that criminal convictions or past misconduct are relevant factors for assessing the suitability of a person. Consideration should also be taken to the lapse of time since the misconduct or conviction, and its severity, as well as the person's subsequent conduct.
- Financial indicators: These provide information on possible financial misconduct, improper conduct in financial accounting, or negligence in decision-making. Indicators could be financial difficulties leading to legal proceedings, a mismatch between financial commitments and income and other funds, personal bankruptcy or financial difficulties, bankruptcy or insolvency proceedings in or in respect of an entity in which the individual is a Board Member, a member of the Senior Management or a Key Person in Control Functions.

- Supervisory indicators: These provide information gathered by or that comes to the attention of supervisors in the performance of their supervisory duties. These supervisors could also be authorities with supervisory responsibility in sectors other than insurance. Indicators could be the withholding of information from public authorities, submission of incorrect financial or other statements, market conduct transgressions, and prior refusal of regulatory approval for relevant positions, other corrective actions or interventions by a public authority.
- Other indicators: These may provide other information relevant to the suitability of the individual. Examples include disputes with previous employers concerning incorrect fulfilment of responsibilities or non-compliance with internal policies, including code of conduct, which led to the lawful dismissal of the person or to the imposition of a penalty under employment law or contract law, and disciplinary measures imposed by trade or professional associations, for example on actuaries, accountants or lawyers. Additionally, strength of character, such as the ability and willingness to challenge, may be an indicator of a person's integrity as well as competence to perform the respective role.

Suitability requirements for Significant Owners

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.

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.

5.3 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.

5.3.1 The supervisor requires the insurer to take the necessary measures to ensure that these requirements are met by setting high internal standards of ethics and integrity, promoting sound corporate governance and requiring that the above-noted individuals have relevant experience, and maintain a sufficient degree of knowledge and decision making ability.

5.3.2 The application of suitability requirements relating to competence for Board Members, Senior Management and Key Persons in Control Functions in an insurer may vary depending on the degree of their influence and on their responsibilities. It is recognised that an individual considered competent for a particular position within an insurer may not be considered competent for another position with different responsibilities or for a similar position within another insurer.

5.3.3 The suitability assessment of Board Members, Senior Management, Key Persons in Control Functions and Significant Owners of an insurer by the supervisor should be conducted as part of the licensing procedure before the insurer is permitted to operate. (ICP 4: Licensing)

When the insurer is already licensed, the supervisor should require the insurer to review and satisfy itself as to the appropriateness of the procedures that are in place within the insurer to perform internal suitability assessments. The supervisor may also require the insurer to certify that it has conducted such assessments and demonstrate how it reached its conclusions.

- 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.

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.

5.4 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.

5.4.1 Insurers should be required to report forthwith any information gained about these persons that may materially adversely affect their suitability.

5.5 The supervisor takes appropriate action to rectify the situation when Board Members, Senior Management and Key Persons in Control Functions or Significant Owners no longer meet suitability requirements.

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.

5.5.2 The supervisor should have the power to impose various measures of a preventive and corrective nature in respect of Significant Owners who do not meet the relevant suitability requirements. Examples of such measures could include the power to require the Significant Owners to dispose of their interests in the insurer within a prescribed period of time, the suspension of the exercise of their corresponding voting rights, or the nullification of any votes cast or the possibility of their annulment.

5.5.3 There can be circumstances where a Board Member, a member of the Senior Management or a Key Person in Control Functions is unable to carry out his/her role and a replacement needs to be appointed on short notice. In jurisdictions where the supervisor approves the post-licensing appointment of Board Members, Senior Management or Key Persons in Control Functions, it may be appropriate, for example for policyholder protection, for the supervisor to permit the post to be filled temporarily until the successor's suitability assessment is affirmed. In such circumstances, a supervisor might require that these temporary replacements meet certain suitability requirements, depending on his/her position or responsibilities within the insurer. However, such assessment should be conducted and concluded with all the deliberate speed.

5.6 The supervisor exchanges information with other authorities inside and outside its jurisdiction where necessary to check the suitability of Board Members, Senior Management, Key Persons in Control Functions and Significant Owners of an insurer.

- 5.6.1 Legislation defines the extent of possible information exchange inside and outside a jurisdiction taking into account confidentiality issues and existing Memoranda of Understanding.
- 5.6.2 The supervisor uses this information as an additional tool to effectively assess the suitability of, or to obtain information on, a Board Member, a member of the Senior Management or a Key Person in Control Functions of an insurer, notably for foreign insurers.
- 5.6.3 If a Significant Owner that is to be assessed is a legal person or a corporate entity regulated in another jurisdiction, the supervisor should seek confirmation from the relevant regulators that the entity is in good standing in that other jurisdiction.

ICP 7 Corporate Governance

The supervisor must require insurers to establish and implement a corporate governance framework which provides for sound and prudent management and oversight of the insurer's business and adequately recognises and protects the interests of policyholders.

Introductory Guidance

- 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 non-compliance or weak oversight, controls or management.
- 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.
- 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.

- 7.0.4 The corporate governance Standards are designed with sufficient flexibility to apply to supervision of insurers regardless of any differences in the corporate structures and legal systems that prevail in the 'jurisdiction of incorporation' or 'domicile of operations' of insurers. The application of corporate governance Standards in this document by both insurers and supervisors should reflect the nature, scale and complexity of the business of the insurer.

One-tier and two-tier Boards

- 7.0.5 While some jurisdictions adopt a one-tier (unicameral) Board system, in other jurisdictions a two-tier (bicameral) Board system is used. In a one-tier system, there is one board comprised of both executive (internal) and non-executive (external or independent) directors. In a two-tier system, there are two boards; i.e. the supervisory or external board (comprised of external independent or non-executive directors) and the management or internal board (comprised of internal or executive directors).

- 7.0.6 A reference to the Board in these Standards, unless otherwise specified, should be taken as a reference to the entire Board. However, in a two-tier system, oversight responsibilities of the Board should generally be applied to the supervisory or external board, whereas the internal board, to the extent it assumes day-to-day management functions of the insurer, shares the responsibilities allocated to the Senior Management. In a one-tier system, the references to the Board and Senior Management follows the oversight and management roles performed by these functions respectively.

Mutuals and co-operatives

- 7.0.7 Governance of insurers formed as mutuals or co-operatives is different from that of insurers formed as joint stock companies (i.e., bodies corporate). In these mutuals and co-operative structures, the insurer is collectively owned (and/or controlled) by policyholders, thereby reducing the divergence of interests that arise in corporate structures between shareholders and policyholders. These Standards are nevertheless sufficiently flexible to be adapted to mutuals and co-operatives to promote the alignment of actions and interests of the Board and Senior Management with the broader interests of policyholders, consistent with sound corporate governance practices. Where there are references to shareholders

or stakeholders, they should be generally treated as references to policyholders in mutuals, unless otherwise indicated.

Group structures

- 7.0.8 Insurance groups should have and implement group-wide governance policies for their subsidiaries. It is expected that where an insurer adopts group-wide corporate governance policies and practices, such group-wide policies and practices should meet the requirements and objectives of these Standards at the legal entity level, taking into account the nature, scale and complexity of the operations of the legal entity and any group-wide risks that affect the entity.

Branch operations

- 7.0.9 If an insurer is a branch operation, these Standards would generally apply to the legal entity in its home jurisdiction. However, the host supervisor may require designated oversight and/or management accountabilities and structures to be maintained at the branch, including in some cases a designated representative responsible for the management of the branch operation. In such cases, these Standards should also apply as appropriate, to the oversight and management roles maintained within the branch operation taking due account of the governance structures and arrangements as determined by the host supervisor.

Remuneration policy and practices

- 7.0.10 Sound remuneration practices are part of sound corporate governance of an insurer. This Standard and guidance are neither intended to unduly restrict nor reduce an insurer's ability to attract and retain skilled talent by prescribing any particular form or level of individual remuneration. Rather, they aim to promote the alignment of remuneration policies with the long term interests of insurers to avoid excessive risk taking, thereby promoting sound overall governance of insurers and fair treatment of customers. The Standard and guidance apply to the supervision of remuneration policies and practices of all insurers, especially where variable remuneration is used, taking into account the nature, scale and complexity of the business of the insurer.

Objectives and strategies of the insurer

- 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.***

- 7.1.1 The Board should adopt a rigorous process for setting (including approving), and overseeing the implementation of, the insurer's overall 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. These objectives and strategies should be adequately documented and properly communicated to its Senior Management, Key Persons in Control Functions and all other relevant staff of the insurer.
- 7.1.2 The Board should take a lead in setting the "tone at the top", including by setting the fundamental corporate values for the insurer. These values should be reflected in the insurer's business objectives and strategies, and be supported by professional standards and codes of ethics that set out what the insurer considers to be acceptable and unacceptable conduct. In this regard, the Board should take account of the nature of the insurer's business and the role it plays in the wider financial system.
- 7.1.3 The Board should ensure that the insurer's overall business objectives and strategies are reviewed at least annually to ensure that they remain appropriate in light of any changes in internal or external business and operating conditions. The Board should ensure more frequent reviews, for instance where an insurer embarks on a significant new business initiative (e.g. a merger or acquisition, or a material change in the direction with respect to the insurer's product portfolio, risk or marketing strategies) the introduction of a new type or class of risk or product or a decision to market products to a new class or category of clients), or following the occurrence of significant external or internal events with the potential to have a material impact on the insurer (including the financial condition, objectives and strategies of the insurer) or the interests of its stakeholders.
- 7.1.4 The Board should establish clear and objective performance goals and measures, both for the insurer and its Senior Management, to promote the effective implementation of the insurer's business objectives and risk strategies, taking due account of, among other things, the insurer's long term interests and viability. Where performance goals and measures are developed by the internal or management board in a two-tier system, the external or supervisory board should review the appropriateness of the goals and measures set. The Board as a whole (i.e. including the external or supervisory board in a two-tier system) should also assess, at suitable intervals, whether those performance goals are achieved against the set performance measures for the Senior Management.

Appropriate allocation of oversight and management responsibilities

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.**

7.2.1 The Board should ensure that the insurer has a well defined governance structure which provides for the effective separation between oversight and management functions. In some jurisdictions, notably those which adopt two-tier systems, such a separation is required by law. The Board is responsible for providing the overall strategy and direction for the insurer and overseeing its proper overall management, while leaving the day-to-day management of the insurer to key executives and management. The separation of the roles of the Chair of the Board and the Chief Executive Officer (CEO) is also commonly used as an effective means for reinforcing a clear distinction between accountability for oversight and management.

7.2.2 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 where they exist, and to the Senior Management and Key Persons in Control Functions to ensure proper oversight of the management of the insurer. The allocation of roles and responsibilities should also clearly identify the individual and collective accountabilities for the discharge of the respective roles and responsibilities.

7.2.3 Where an insurer has a one-tier Board comprising both executive and non-executive directors, the allocation of responsibilities to individual Board members (for example the membership of certain committees of the Board such as the audit or remuneration committee) 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. As non-executive members of the Board are not involved in the day-to-day management of the insurer, they are more suited to perform the effective oversight of the executive functions. In two-tier systems, the allocation of responsibilities to individuals should similarly reflect the roles played by such individuals as members of the supervisory or executive boards.

7.2.4 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, and by being actively involved in such processes;

- monitor whether the Senior Management is managing the affairs of the insurer in accordance with the strategies and policies set by the Board, including the insurer's risk appetite, and meeting the performance goals set by the Board; and
- regularly meet with the Senior Management to discuss and review critically the decisions made, information provided and any explanations given by the Senior Management relating to the business and operations of the insurer.

7.2.5 As a part of its regular monitoring and review of the insurer's operations, the Board should review whether the policies and procedures, as set by the Board, are being properly implemented, and are operating as intended. Particular attention should be paid as to whether the responsibilities for managing and implementing the policies of the Board have been effectively discharged by those responsible. The Board should obtain reports at least annually for this purpose and such reports may include internal or external independent reports as appropriate.

Structure and governance of the Board

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.**

Board composition

7.3.1 Depending on the nature, scale and complexity of its operations, the Board of an insurer should have a sufficient number of members who have relevant expertise among them as necessary to provide effective leadership, direction and oversight of the insurer's business to ensure it is conducted in a sound and prudent manner. For this purpose, 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 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.

- 7.3.2 Board members should meet the suitability requirements set out in *ICP 5: Suitability of Persons*. In addition, they should have the commitment necessary to fulfil their roles, demonstrated by, for example, a sufficient allocation of time to the affairs of the insurer and reasonable limits on the number of external Board memberships held.
- 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.

Board effectiveness

- 7.3.4 The Board should review, at least annually, its own performance to ascertain whether members collectively and individually remain effective in discharging the respective roles and responsibilities assigned to them, and identify opportunities to improve the performance of the Board as a whole. The Board should implement appropriate measures to address any identified inadequacies, including any training programmes for Board members. The Board may also consider the use of external expertise from time to time to undertake its performance assessment where appropriate in order to enhance the objectivity and integrity of that assessment process.

Internal governance

- 7.3.5 The Board should have appropriate practices and procedures for its own internal governance, and ensure that these are followed, and periodically reviewed to assess their effectiveness and adequacy. These may be included in organisational rules or by-laws, and should set out how the Board will carry out its roles and responsibilities. They should also cover a formal and documented process for nomination, selection, and removal of Board members, and a specified term of office as appropriate to the roles and responsibilities of the Board member, particularly to ensure the objectivity of decision making and judgement. Appropriate succession planning should also form part of the Board's internal governance practices.

Chair of the Board

- 7.3.6 While the Board as a whole remains collectively responsible for the stewardship of the insurer, 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 responsibilities such as setting the Board's agenda, ensuring that there is adequate time allocated for the discussion of agenda items, especially if they involve strategic or policy decisions of significant importance, and for promoting a culture of openness and debate, by facilitating effective participation of, and communication between, non-executive and executive members, and also with the Senior Management and Key Persons in Control Functions.

Board Committees

- 7.3.7 To support the effective discharge of the responsibilities of the Board, the Board should assess whether the establishment of committees of the Board is appropriate. Committees that a Board may commonly establish, depending on the nature, scale and complexity of operations of the insurer, include the audit, remuneration, ethics/compliance, nominations and risk management committees. Where committees are appointed, they should have clearly defined mandates, authority to carry out their respective functions, and the degree of independence and objectivity as appropriate to the role of the committee. If the functions of any committees are combined, the Board should ensure such a combination does not compromise the integrity or effectiveness of the functions combined. In all cases, the Board remains ultimately responsible for matters delegated to any such committees.

Independence and objectivity

- 7.3.8 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 by the Board. For this purpose, the independence criteria should also take account of group structures and other relevant factors. Meeting such criteria is particularly important for those Board members undertaking specific roles (such as members of the remunerations and audit committees) in which conflicts of interests are more likely to arise. Board members should also bear in mind the duties of good faith and loyalty applicable to them at the individual level, as set out in Standard 7.4.

Board powers

- 7.3.9 To be able to discharge its role and responsibilities properly, the Board should have well-defined powers, which are clearly set out either in the legislation or as part of the constituent documents of the insurer (such as the constitution, articles of incorporation and organisational rules). These should, at a minimum, include the power to obtain timely and comprehensive information relating to the management of the insurer, including direct access to relevant persons within the organisation for obtaining information such as the Senior Management and Key Persons in Control Functions.

Access to resources

- 7.3.10 Funding and other resources should be allocated to the Board to enable the Board members to carry out their respective roles and responsibilities efficiently and effectively. The Board should have access to services of external consultants or specialists where necessary or appropriate, subject to due procedures for appointment and dismissal of such consultants or specialists.

Delegations

- 7.3.11 The Board may, as appropriate to the nature scale and complexity of the insurer's business, delegate some of the activities or tasks associated with its own roles and responsibilities. (Delegations in this context are distinguished from outsourcing of business activities by the insurer, which are dealt with in *ICP 8: Risk Management and Internal Controls*.) Notwithstanding such delegations, the Board as a whole retains the ultimate responsibility for the activities or tasks delegated, and the decisions made in reliance on any advice or recommendations made by the persons or committees to whom the tasks were delegated. Where the Board makes any delegations, it should ensure that:

- the delegation is appropriate. Any delegation that results in the Board not being able to discharge its own roles and responsibilities effectively would be an undue or inappropriate delegation. For example, the duty to oversee the Senior Management should not be delegated to a Board committee comprised mostly or solely of executive members of the Board who are involved in the day-to-day management of the insurer;
- the delegation is made under a clear mandate with well defined terms such as those relating to the powers, accountabilities and procedures relating to the delegation, and is supported by adequate resources to effectively carry out the delegated functions;

- there is no undue concentration of powers giving any one person or group of individuals unfettered and inappropriate level of powers capable of influencing the insurer's business or management decisions;
- it has the ability to monitor and require reports on whether the delegated tasks are properly carried out; and
- it retains the ability to withdraw the delegation if it is not discharged properly and for due purposes by the delegate, and for this purpose, have appropriate contingency arrangements in place.

Duties of individual Board members

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.**

7.4.1 The specific duties identified above are designed to address conflicts of interests that arise between the interests of the individual members of the Board and those of the insurer and policyholders. The insurer should include these duties as part of the Board charter or mandate containing the terms of engagement of the individual Board members.

7.4.2 The supervisor should be satisfied that individual Board members understand the nature and scope of their duties and how they impact on the way in which the member discharges his/her respective roles and responsibilities. A Board member should consider his/her ability to discharge the roles and responsibilities in a manner as would be expected of a reasonably prudent person placed in a similar position. He/she should act on a fully informed basis, and for this purpose continually seek and acquire information as necessary.

7.4.3 Where a member of the Board of an insurer has common membership on the Board of any other entity within or outside the insurer's group, there should be clear and well defined procedures that require the member of the insurer's Board to act in the best interests of the insurer, putting the insurer's and policyholders

interests ahead of that of any other entity or that of his/her own. These may include appropriate disclosure and in some instances shareholder approval of such overlapping roles. In the event of a material conflict with the interests of the insurer, the member should disclose such conflicts promptly to the Board of the insurer and its stakeholders as appropriate, and be required to decline to vote or take any decisions in any matters in which he/she has an interest.

Risk management and internal control systems and functions

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.

7.5.1 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 8: Risk Management and Internal Controls* sets out the elements of these systems and functions. These systems and functions should cover not only prudential risks but also conduct of business risks, which are described in *ICP 19: Conduct of Business*.

Remuneration policy and practices

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”).**

Overall remuneration strategy and oversight

7.6.1 As a part of effective risk management, an insurer should adopt and implement a prudent and effective remuneration policy. Such a policy should not encourage individuals particularly Board members, senior managers, Key Persons in Control Functions and “major risk-taking staff” to take inappropriate or excessive risks, especially where performance based variable remuneration is used.

- 7.6.2 The Board, particularly members of the 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. Such competencies include things such as a sufficient understanding of the relationship between risk and remuneration practices. The remuneration committee, where established, should have an adequate representation of independent non-executive members to promote objectivity in decision-making.
- 7.6.3 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. For this purpose, appropriate consideration should be given by the Board to relevant elements of the remuneration policy and structure, 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.
- 7.6.4 The Board should ensure that in structuring, implementing and reviewing the insurer's remuneration policy, the decision-making process identifies and manages conflicts of interests and is properly documented. Any member of the Board should not be placed in a position of actual or perceived conflicts of interests in respect of remuneration decisions.
- 7.6.5 The Board should also ensure that relevant Key Persons in Control Functions are involved in the remuneration policy-setting and monitoring process to ensure that remuneration practices do not create incentives for excessive or inappropriate risk taking, are carried out consistently with established policies and promote alignment of risks and rewards across the organisation. Similarly, the remuneration and risk management committees of the Board, if such committees exist, should interact closely with each other and provide input to the Board on the incentives created by the remuneration system and their effect on risk-taking behaviour.
- 7.6.6 The potential for conflicts of interests that may compromise the integrity and objectivity of the staff involved in control functions,

should be mitigated. This can be achieved by a variety of means, such as making their remuneration:

- predominantly based on the effective achievement of the objectives appropriate to such control functions. Performance measures for staff in control functions should represent the right balance between objective assessments of the control environment (e.g. the conduct of the relationship between the control functions and executive management) and outputs delivered by the control functions, including their impact, quality and efficiency in supporting the oversight of risks. Such output measures may include recommendations made and implemented to reduce risks, reduction in number of compliance breaches and measures adopted to promptly rectify identified breaches, results of external quality reviews, and losses recovered or avoided through audits of high risk areas;
- not linked to the performance of any business units which are subject to their control or oversight. For example, where risk and compliance functions are embedded in a business unit, a clear distinction should be drawn between the remuneration policy applicable to staff undertaking control functions and other staff in the business unit, such as through the separation of the pools from which remuneration is paid to the two groups of staff; and
- adequate as an overall package to attract and retain staff with the requisite skills, knowledge and expertise to discharge those control functions effectively and to increase their competence and performance.

7.6.7 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.

Variable remuneration

7.6.8 Variable remuneration should be performance-based using measures of individual, unit or group performance that do not create incentives for inappropriate risk taking.

7.6.9 To better align performance-based incentives with the long term value creation and the time horizon of risks to which the insurer may be exposed, due consideration should be given to the following:

- There should be an appropriate mix of fixed and variable components, with adequate parameters set for allocating

cash versus other forms of remuneration, such as shares. A variable component linked to performance that is too high relative to the fixed component may make it difficult for an insurer to reduce or eliminate bonuses in a poor financial year.

- The reward for performance should include an adjustment for the material current and future risks associated with performance. Since the time horizon of performance and associated risks can vary, the measurement of performance should, where practicable, be set in a multi-year framework to ensure that the measurement process is based on longer term performance;
- If the variable component of remuneration is significant, the major part of it should be deferred for an appropriate specified period. The deferral period should take account of the time frame within which risks associated with the relevant performance (such as the cost of capital required to support risks taken and associated uncertainties in the timing and the likelihood of future revenues and expenses) may materialise. The deferral period applied may vary depending on the level of seniority or responsibility of the relevant individuals and the nature of risks to which the insurer is exposed;
- The award of bonuses should contain provisions that enable the insurer, under certain circumstances, to apply malus or claw back arrangements in the case of subdued or negative financial performance of the insurer which is attributed to the excessive risk taking of the staff concerned; and
- Guaranteed bonuses should generally not be offered, as they are not consistent with sound risk management and performance based rewards.

7.6.10 The variable component should be subject to prudent limits set under the remuneration policy that are consistent with the insurer's capital management strategy and its ability to maintain a sound capital base taking account of the internal capital targets or regulatory capital requirements of the insurer.

7.6.11 The performance criteria applicable to the variable components of remuneration should promote a complete assessment of risk-adjusted performance. For this purpose, due consideration should be given to the need for performance criteria to:

- be clearly defined and be objectively measurable;

- be based not only on financial but also on non-financial criteria as appropriate (such as compliance with regulation and internal rules, achievement of risk management goals as well as compliance with market conduct standards and fair treatment of policyholders and claimants);
- take account of not only the individual's performance, but also the performance of the business unit concerned where relevant and the overall results of the insurer and the group; and
- not treat growth or volume as a criterion in isolation from other performance criteria.

Share-based components

7.6.12 Where share-based components of variable remuneration (such as shares, share options or similar instruments) are used, appropriate safeguards should be implemented to align incentives and the longer-term interests of the insurer. Such safeguards may include that:

- shares do not vest for a minimum specified period after their award ("vesting restrictions");
- share options or other similar rights are not exercisable for a minimum specified period after their award ("holding restrictions"); and
- individuals are required to retain an appropriate proportion of the shares awarded until the end of their employment or other specified period beyond their employment ("retention restrictions").

7.6.13 Subject to any applicable legal restrictions, it is appropriate that future vesting and holding restrictions for share-based remuneration remain operative even upon cessation of employment (i.e. there should be no undue acceleration of the vesting of share-based payments or curtailing of any holding restrictions).

Severance payments

7.6.14 Where an insurer provides discretionary payouts on termination of employment ("severance payments"), sometimes also referred to as "golden parachutes", such payment should generally be subject to appropriate governance controls and limits. In any case, such payouts should be aligned with the insurer's overall financial condition and performance over an appropriate time horizon. Severance payments should generally not be payable in the case of

failure or threatened failure of the insurer, particularly to an individual whose actions have contributed to the failure or potential failure of the insurer.

Reliable and transparent financial reporting

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.

7.7.1 The Board is responsible for having adequate systems and controls to ensure that the financial reports of the insurer present a balanced and accurate assessment of the insurer's business and its general financial health and viability as a going concern. In discharging this responsibility, the Board should carry out specific oversight functions. To increase its effectiveness, many insurers have an Audit Committee of the Board for this purpose. Where this is not practicable, the Board, as a whole, carries out these 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 (encompassing external audit and reviews by internal audit of the insurer's financial reporting controls), and reviewing the auditor's plans and material findings;
- overseeing the processes for hiring, removing, and assessing the performance and independence of the external auditor to ensure the appointed external auditor has the necessary knowledge, skills, expertise, integrity and resources to conduct the audit;
- 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 (by the Audit Committee where one is established) and the supervisor on significant issues concerning the financial reporting process, including the circumstances relating to the resignation or removal of the external auditor and the actions taken to address or mitigate identified financial reporting risks.

7.7.2 It is particularly important that the Board safeguards and promotes an effective relationship with the external auditor and for this purpose ensures 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 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, including policies and processes that address the auditor's compliance with applicable ethical and professional standards, restrictions and conditions for the provision of non-audit services which are subject to approval by the Board, partner or firm periodic rotation as appropriate, and safeguards to eliminate or reduce to an acceptable level identified threats to 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 an extension of the audit engagement;
- there is unrestricted access by the external auditor to information and persons within the insurer as necessary to conduct the audit; and
- there is an evaluation of the effectiveness of the external audit process at the end of the audit cycle.

7.7.3 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 Board should require that any information regarding internal control weaknesses or deficiencies which the external auditor becomes aware of, is promptly communicated to the Board. Appropriate actions should be taken by the Board where doubts arise as to the reliability of the external auditor's opinion as an independent attestation of the insurer's internal financial reporting and control processes.

- 7.7.4 There should be regular meetings between the Board and the external auditor during the audit cycle, including meetings without management present.
- 7.7.5 The supervisor should require that it be notified by the external auditor of material fraud, suspicion of material fraud and regulatory breaches or other significant audit findings identified in the course of the audit. Copies of reports prepared by the external auditor for the insurer (e.g. such as management letters) should be extended to the supervisor. Such information should be provided to the supervisor without the need for prior consent of the insurer and the external auditor should be duly protected from liability for any information so disclosed to the supervisor in good faith.
- 7.7.6 The supervisor should have, and exercise, the power to require a further audit by a different external auditor or to have the auditor replaced where necessary.
- 7.7.7 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.

Transparency and communications

- 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.**
- 7.8.1 Communications with the supervisor and other stakeholders should promote effective engagement of the supervisor and stakeholders on the governance of the insurer to enable informed judgements about the effectiveness of the Board and Senior Management in governing the insurer.
- 7.8.2 Subject to any reasonable commercial sensitivities and applicable privacy or confidentiality obligations, the insurer's communication policies and strategies should include providing to the insurer's stakeholders information such as the following:
- the insurer's overall strategic objectives, covering existing or prospective lines of business and how they are being or will be achieved;
 - the insurer's governance structures, such as allocation of oversight and management responsibilities between the Board and the Senior Management, and organisational structures, including reporting lines;

- members of the Board and any Board committees, including their respective expertise, qualifications, track-record, other positions held by such members, and whether such members are regarded as independent;
- processes in place for the Board to evaluate its own performance and any measures taken to improve the Board's performance;
- the general design, implementation and operation of the remuneration policy;
- major ownership and group structures, and any significant affiliations and alliances; and
- material related-party transactions.

7.8.3 The supervisor may require more detailed and additional information relating to the insurer's corporate governance for supervisory purposes, which may include commercially sensitive information, such as assessments by the Board of the effectiveness of the insurer's governance system, internal audit reports, and more detailed information on the remuneration structures adopted by the insurer for the Board, Senior Management, Key Persons in Control Functions and major risk-taking staff. The insurer's communication policies and strategies should enable such information to be provided to the supervisor in a timely and efficient manner. Supervisors should safeguard such information having due regard to the confidentiality of commercially sensitive information and applicable laws.

7.8.4 Disclosures of information on remuneration should be sufficient to enable stakeholders to evaluate how the remuneration system relates to risk and whether it is operating as intended. Relevant information may include:

- the operation of risk adjustments, including examples of how the policy results in adjustments to remuneration for employees at different levels;
- how remuneration is related to performance (both financial and personal business conduct) over time; and
- valuation principles in respect of remuneration instruments.

7.8.5 Appropriate quantitative information should also be made to enable supervisors and stakeholders to evaluate the financial impact of the remuneration policy. Such information may include:

- the total cost of remuneration awarded in the period, analysed according to the main components such as basic salary, variable bonus and long-term awards;
- the total amount set aside in respect of deferred remuneration;
- adjustment to net income for the period in respect of remuneration awarded in previous periods;
- the total costs of all sign-on payments in the period and number of individuals to whom these relate; and
- the total costs of all severance payments in the period and number of individuals to whom these relate.
- These amounts should be analysed by type of instrument (e.g. cash, shares, share options etc.) as applicable, and in a manner consistent with the key elements of the remuneration policy.

7.8.6 Disclosure of information on governance should be made on a regular (for instance, at least annually) and timely basis.

Duties of the Senior Management

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.**

7.9.1 Senior Management should implement appropriate systems and controls to ensure that they can effectively carry out the day-to-day management of the business of the insurer in order to achieve the insurer's business objectives and strategies, and in particular in accordance with the established levels of risk appetite and consistent with internal policies. Such systems and controls should encompass:

- clear and transparent process for engaging persons with appropriate competencies and integrity to discharge the functions of the Senior Management, which include succession planning, on-going training and procedures for termination;
- clear lines of accountability and channels of communication between persons undertaking Senior Management and Key Persons in Control Functions;
- proper procedures for the delegation of Senior Management functions and monitoring whether delegated functions are carried out effectively and properly, in accordance with the same principles that apply to delegations by the Board (see Guidance under 7.3.11);
- standards of conduct and codes of ethics for the Senior Management and other staff to promote a culture of sound risk management and compliance, which include procedures for dealing with conflicts of interests, and the effective implementation on an on-going basis of such standards and codes (see ICP 8: *Risk Management and Internal Controls* for conflicts of interest provisions);
- proper channels of communications, including clear lines of reporting, as between the individuals performing the functions of the Senior Management and the Board, including provisions dealing with whistleblower protection, and their effective implementation; and
- effective communication strategies with supervisors and stakeholders that include the identification of matters that should be disclosed, and to whom such disclosure should be made.

7.9.2 Senior Management should also ensure that there are adequate procedures for assessing the effectiveness of their performance against the performance objectives set by the Board. For this purpose, they should carry out at least an annual assessment of their own performance against set goals. Any identified inadequacies or gaps should be addressed promptly and reported to the Board.

7.9.3 Senior Management should also promote strong internal controls. It should not interfere with the activities that control functions carry out in the rightful exercise of their responsibilities, including that of providing an independent view of governance, risk, compliance and control related matters.

Supervisory review

7.10 The supervisor has the power to require the insurer to demonstrate the adequacy and effectiveness of its corporate governance framework.

- 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 off-site) 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.
- 7.10.2 The onus for demonstrating, to the satisfaction of the supervisor, that the corporate governance framework is effective and operates as intended rests with the insurer. The supervisor should provide any guidance and rulings as appropriate to facilitate this process. The supervisor should, for the purposes of monitoring due compliance, establish effective channels of communication with the insurer, and have access to relevant information concerning the governance of the insurer. This may be obtained through periodic reports to the supervisor and any information obtained on an ad-hoc basis (see also 7.8).
- 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.
- 7.10.4 To ascertain the on-going effectiveness of the Board in light of the nature, scale and complexity of the insurer's operations, the supervisor may also consider the use of measures such as the following where appropriate:

- on-going mandatory training for Board members that is commensurate with their respective duties, roles and responsibilities within the insurer;
- a review of the periodic self-evaluation undertaken by the Board as referred to in paragraph 7.3.5;
- meetings and/or interviews with the full Board and its individual members as appropriate, particularly to reinforce the expectations placed on Board members relating to their performance and to get a sense of how informed and proactive they are; and
- attending and observing Board proceedings.

7.10.5 Where remuneration policies of an insurer contain more high risk elements, closer supervisory scrutiny of those policy and practices may also be warranted, including requests for additional information as appropriate to assess whether those practices are having an adverse impact on the on-going viability of the insurer or commissioning an independent assessment of the insurer's remuneration policy and practices.

ICP 8 Risk Management and Internal Controls

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.

Introductory Guidance

- 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.
- 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.
- 8.0.3 The exact nature of the *systems* that the Supervisor requires the insurer to have is dependent on many factors. These include whether the insurer belongs to the category of insurers identified by the Financial Stability Board as requiring more intense supervision, the insurer's risk profile, and the applicable legal and regulatory requirements. These systems typically include:
- *strategies* setting out the approach of the insurer for dealing with specific areas of risk and legal and regulatory obligation;
 - *policies* defining the procedures and other requirements that employees need to follow;
 - *processes* for the implementation of agreed strategies and policies;
 - *controls* to ensure that such strategies, policies and processes are in fact in place, are being observed, and are attaining their intended objectives.
- 8.0.4 The risk management system of an insurer comprises the totality of strategies, policies, and processes, for identifying, assessing, monitoring, managing and reporting risks to which the insurer may be exposed at an individual and at a consolidated level.

- 8.0.5 The totality of all controls an insurer has in place is generally referred to as the *internal controls system*.
- 8.0.6 An insurer also has properly authorized functions (whether in the form of a person, unit or department) to carry out specific activities relating to matters such as risk management, compliance, actuarial matters, and internal audit. These are generally referred to as control functions.

Special Considerations for Groups

- 8.0.7 Adequate governance, risk management and internal controls should be in place within the group. These should be assessed by the supervisor on a group-wide basis and on a solo basis to have a group view and enhance the assessment of the solo entities.
- 8.0.8 Groups may adopt different types of management structures. In some groups, the management structure may correspond closely to the legal entity structure, while in others the organization may be by lines of business or geographically structured. The supervisor should take the management structure of the group into consideration. When business activities and risks are managed independently of legal entities, it is not sufficient to assess governance or risk only at the individual insurer level. Control Functions and the supervisor need to be able to establish, with a reasonable level of assurance, that appropriate governance exists across the group and that risks are being identified, assessed, monitored and managed appropriately also on a group-wide basis and that the soundness of the group and each insurer within the group is secured.
- 8.0.9 Even where each insurer within the group is independently managed, its respective decisions, as well as its governance, risk management, and internal controls, may have consequences for the group as a whole and for other individual entities within the group. Appropriate assessment of these on a group-wide basis is still important.
- 8.0.10 Being part of a group may enable some insurers to underwrite larger amounts of risks and risks of higher magnitude than would be possible on a stand-alone basis. Whether or not appropriate risk mitigation arrangements (e.g. reinsurance) are in place, it is important that the role of each insurer within the group is clearly defined and that clear limits on the risk taken by each insurer are established.
- 8.0.11 In the above context, it is important to ensure that, group-wide as well as on legal entity, or line of business basis, Senior Management and the Board of Directors at the head of the group

have relevant and timely information for their respective decision making processes.

Systems for Risk Management and Internal Controls

8.1 The Supervisor requires an insurer to establish, and operate within, an effective system of risk management and of internal controls.

Basic Components of a Risk Management System

- 8.1.1 The ultimate responsibility for ensuring that an effective risk management system is in place lies with the Board of Directors.
- 8.1.2 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.
- 8.1.3 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 categorization 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.

Scope and Embedding of the Risk Management System

- 8.1.4 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.
- 8.1.5 The risk management system should be integrated into the culture of the insurer and into the various business areas and units of the insurer such as to have the appropriate risk management practices and procedures embedded in the key operations and structures of the insurer company-wide.
- 8.1.6 The insurer's risk policies should be written in a way to help employees understand their risk responsibilities. They should also help explain the relationship of the risk management system to the insurer's overall governance framework and to its corporate culture.
- 8.1.7 Regular communications and training on the risk policies should take place.
- 8.1.8 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.
- 8.1.9 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 control functions. Any proposed activity that would go beyond the Board-approved risk appetite should be subject to appropriate review and require Board approval.

- 8.1.10 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.
- 8.1.11 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.
- 8.1.12 Material changes to an insurer's risk management system should be documented and subject to approval by the Board. The reasons for the changes should be documented. Appropriate documentation should be available to internal audit, external audit, and the supervisor for their respective assessments of the risk management system.

Internal Controls System

- 8.1.13 The ultimate responsibility for ensuring that an adequate and effective Internal Controls System (ICS) is in place lies with the Board of Directors.
- 8.1.14 The ICS should be designed and operated to assist the Board of Directors and Senior Management in the fulfillment of their respective responsibilities for oversight and management of the company. The ICS provides 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.
- 8.1.15 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 control³ of an insurer, as well as all its controls cumulatively, should be designed for effectiveness and operate effectively.
- 8.1.16 In fulfilling its responsibility in respect of the ICS, the Board of Directors reviews and approves the organisational and other measures regarding internal controls. The goal is a coherent system where the controls form a rational insurer-wide framework (from

³Individual controls may be preventive (applied to prevent undesirable outcomes) or detective (to uncover undesirable activity). Individual controls may be manual (human), automated, or a combination thereof and may be either general or process or application specific. Further classification of controls is sometimes used such as distinguishing between controls that apply to inputs or to outputs and between key and other controls.

process or transactional level, to entity level, to group level) which can be optimized for maximum effectiveness and efficiency.

- 8.1.17 The Board has an overall understanding of the control environment across the various entities and businesses and requires Senior Management to ensure that for each key business process and policy, and related risks and obligations, there is an appropriate control.
- 8.1.18 In addition, the Board of Directors ensures there is clear allocation of responsibilities within the insurer, with appropriate segregation, in respect of the design, documentation, operation, monitoring, and testing of internal controls.⁴
- 8.1.19 The Board of Directors determines which function or functions report to it or to one of its committees in respect of the internal controls system.
- 8.1.20 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, including an analysis on the appropriateness of those resources in light of nature, scale and complexity of the insurer's business, risks and obligations;
 - an assessment of how the various organizational 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 (including any identified by the internal or external auditors or the regulator) and the responses thereto (in each case to the extent not already covered in other reporting made to the Board).

⁴ Appropriate segregation of duties is a fundamental building block of an internal control system. Some companies in some jurisdictions allocate responsibilities according to the concept of "lines of defense" such as in considering management as the "first line of defense", the control functions (other than internal audit) as the "second line of defense", and internal audit as the "third line of defense". Management is deemed to "own" the controls and the other "lines of defense" are there to help ensure their application and viability. Whatever approach is used, it is important that responsibilities be allocated to promote checks-and-balances and avoid conflicts of interest. Responsibilities should be properly documented, such as in charters, authority tables, or other similar governance documents.

8.1.21 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 includes 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, including the reporting made to the insurer's regulators;
- appropriate controls for other key business processes and policies, including for major business decisions and transactions (including insurer-internal 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. Appropriate segregation of duties means, among other things, having sufficient distance between those accountable for a process or policy and those who check if for such process or policy an appropriate control exists and is being applied. It also includes appropriate distance between those who design a control or operate a control and those who check if such control is effective in design and operation;⁵
- 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. Such policies and controls should be designed, among other things, to prevent any major transaction being entered into without appropriate governance review or by anyone lacking the necessary authority and to ensure that borrowing, trading, risk and other such limits are strictly observed. Such policies should foresee a role for control functions, for example by requiring for major matters the review and sign-off by Risk Management or Compliance, and/or approval by a Board level committee;
- controls at the appropriate levels so as to be effective, including at the process or transactional level, at the entity

⁵ It is not inconsistent with good practice, and indeed in some situations desirable, if managers responsible for a business process are allowed to apply certain self-controls and do certain self-assessments at their level, as long as there is a separate review of those controls from an independent control function.

level (whether legal entity or business area level), and, in the case of groups, at the group level;

- a centralized 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. As part of such review, individual controls are monitored and analyzed periodically to determine gaps, redundancies and other improvement opportunities, with Senior Management taking such measures as are necessary to address these;
- 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.

Control Functions (General)

8.2 The Supervisor requires the insurer to have effective control functions with the necessary authority, independence, and resources.

- 8.2.1 As part of an effective system of risk management and internal controls, insurers have control functions, including for risk management, compliance, actuarial matters and internal audit. While Senior Management has primary responsibility for executing in respect of risk, compliance and related areas, specific control functions are essential for providing expertise, leadership, objectivity and independence where required on these subjects. Control functions add to the governance checks-and-balances of the insurer and are a source of support for the Board of Directors in the fulfillment of its risk, compliance, and control oversight duties.
- 8.2.2 A control function should be led by a person of appropriate seniority and expertise.
- 8.2.3 The appointment, performance assessment, remuneration, disciplining and dismissal of the head of each control function (other than the head of the internal audit function 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. While Senior Management may provide input, the appointment and the annual or other periodic performance assessment of the head of the internal audit function is done by the Board of Directors (or its Chair or by the Audit Committee) which solely determines his or her salary, bonus, and any promotions, demotions, or disciplinary actions.

- 8.2.4 The existence of any control function does not relieve the Board of Directors or Senior Management from their respective governance and related responsibilities.
- 8.2.5 Insurers should position each control function and its associated reporting lines into the insurer's organizational structure in a manner that enables such function to operate and carry out its responsibilities effectively.
- 8.2.6 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.
- 8.2.7 To achieve optimisation and provide additional checks and balances, some insurers (particularly larger more complex insurers) have a designated person or function to support the advancement, coordination and/or management of the overall internal controls system on a more regular basis (such as an ICS Manager or similar). Unlike the internal or external auditor who may from time to time test certain controls or periodically opine formally on the existence or effectiveness of the ICS and who thus must have more operational distance, the ICS Manager or similar is closer to the operations of the insurer and helps ensure that appropriate documented controls are in place for the appropriate areas and at the appropriate levels, locally and company-wide.
- 8.2.8 Subject to supervisor approval where required, an insurer may combine certain control functions or outsource a control function in whole or in part where appropriate in light of the nature, scale, and complexity of the insurer's business, risks, and legal and regulatory obligations. In cases where an insurer combines or outsources a control function, or part thereof, the Board of Directors satisfies itself that this does not interfere with the function's independence, objectivity, or effectiveness. The Board approves and reviews periodically any arrangement for combining or outsourcing control functions, including by getting direct input from the relevant control function(s).

Authority and Independence of Control Functions

- 8.2.9 Each control function should have the necessary authority and independence to be effective in fulfilling its duties and attaining its goals.
- 8.2.10 The Board of Directors should set or approve the authority and responsibilities of each control function.
- 8.2.11 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. The head of each control function should periodically review such document and submit suggestions for any changes to Senior Management and the Board of Directors for approval.
- 8.2.12 The independence from Senior Management and from other functions of each control function should be sufficient to allow its staff to (a) serve as a further component of the insurer's checks-and-balances, (b) provide an objective perspective on strategies, issues, and potential violations related to their areas of responsibility, and (c) implement or oversee the implementation of corrective measures where necessary.
- 8.2.13 Each control function should avoid conflicts of interest. Where any conflicts remain and cannot be resolved with Senior Management, these should be brought to the attention of the Board of Directors for resolution.
- 8.2.14 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. In addition control functions should have appropriate access to Senior Management and report to it periodically.

Board Access and Reporting by the Control Functions; Board Assessment of Control Functions

- 8.2.15 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.
- 8.2.16 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.

- 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.

Resources and Qualifications of the Control Functions

- 8.2.18 Each control function should have the resources necessary to fulfill its responsibilities and achieve the specific goals in its areas of responsibility. This includes qualified staff and appropriate IT/management information systems. The function should be organized in a manner appropriate to achieve its goals.
- 8.2.19 The head of each control function should review regularly with Senior Management the adequacy of the function's resources and request adjustments as necessary. Where he or she has a major difference of opinion with Senior Management on resources needed, such person brings the issue to the Board of Directors for resolution. In the case of the internal audit function, the common practice is for its budget and resources to be determined by the Board Audit Committee or the full Board.
- 8.2.20 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. Higher expectations apply to the head of each control function. To ensure that members of each control function remain up to date on the developments and techniques related to their areas of responsibility, they should receive regular training relevant to their field and areas of responsibilities.

Risk Management Function

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

- 8.3.1 A robust risk management function that is well positioned, resourced, and properly authorized and staffed is an essential element of an effective risk management system. Within some insurers, and particularly at larger or more complex ones, such function is led by a Chief Risk Officer or similar.

Access and Reporting to the Board by the Risk Management Function

- 8.3.2 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.

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.

Main activities of the Risk Management Function

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 at a solo and at the group level;

- 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.

Compliance Function

8.4 The supervisor requires the insurer 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.

- 8.4.1 The Board of Directors ensures that the insurer, through the adoption of a code of conduct or other appropriate means, is committed to complying with all applicable laws and regulations, supervisory decisions, and internal policies, and to conduct its business ethically and responsibly.
- 8.4.2 As part of this commitment, the Board should ensure that the insurer has in place a robust and well positioned, resourced, and properly authorized compliance function. Within some insurers, particularly at larger or more complex ones, such function is led by a Chief Compliance Officer.

Board Access and Reporting of the Compliance Function

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

- the strategy (e.g. mission, longer-term goals, overall strategy for achieving these goals) of the compliance function;
- the compliance function's operational plan, including specific annual or other short-term goals being pursued and the performance against such goals;
- information on its resources (personnel, budget, etc.), including an analysis on the appropriateness of those 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 (e.g. divisions, major business units, product areas, etc.) 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.

8.4.4 The head of the compliance function should have the authority and obligation to promptly inform the Chair of the Board directly 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 if in either case he or she believes that Senior Management or other persons in authority at the insurer are not taking the necessary corrective actions and a delay would be detrimental to the insurer or its policyholders.

Main activities of the Compliance Function

8.4.5 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; this includes communicating and holding training on an appropriate code of conduct or similar that incorporates the corporate values of the insurer, aims to promote a high level of professional conduct of the business, and sets out the key conduct expectations of employees;
- identify, assess, report on, and address key legal and regulatory obligations and the risks associated therewith, including obligations to the insurer's supervisor; such analyses should use risk and other appropriate methodologies;
- 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; this includes ensuring there are appropriate means for such reporting;
- address compliance shortcomings and violations, including ensuring that adequate disciplinary actions are taken where appropriate and any necessary reporting to the supervisor or other authorities is made; and
- conduct regular assessments of the compliance function and the compliance policies and systems and implement or monitor needed improvements.

Actuarial Function

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.

- 8.5.1 A robust actuarial function that is well positioned, resourced, and properly authorized and staffed is essential for the proper operation of the insurer.
- 8.5.2 The supervisor should have or have access to the appropriate skills, knowledge and resources to enable it to critically assess the work of an insurer's actuarial function.

Board Access and Reporting of the Actuarial Function

- 8.5.3 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.
- 8.5.4 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.

Main Activities of the Actuarial Function

- 8.5.5 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 utilizing 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.

8.5.6 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.

8.5.7 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.

Appointed Actuary

8.5.8 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.

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

8.5.10 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.

8.5.11 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.

- 8.5.12 The supervisor should have the authority to require an insurer to replace an Appointed Actuary when such person fails to adequately perform required functions or duties, is subject to conflicts of interest, or no longer meets the jurisdiction's requirements to be eligible for the position.

Internal Audit Function

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.

- 8.6.1 Part of the oversight role of the Board of Directors is to ensure there are means for it to receive independent assurance from an internal function that is not operationally involved in the business and is not subject to any conflicts of interest.

- 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 fulfill its mission, in accordance with its charter, terms of reference, or other documents setting out its authority and responsibilities.

Authority and independence of the Internal Audit Function

- 8.6.3 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.

8.6.4 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.

Board Access and Reporting of the Internal Audit Function

8.6.5 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:

- 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.

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

Main activities of the Internal Audit Function

- 8.6.7 The audit function should carry out such activities as are needed to fulfill 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 organizational unit basis;
- reviewing levels of compliance by employees and organizational 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 processes;
- monitoring and evaluating the effectiveness of the organization'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.

8.6.8 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.

8.6.9 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.

Outsourcing of Material Functions or Activities

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.

- 8.7.1 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.
- 8.7.2 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.
- 8.7.3 The Board or Senior Management should be required to satisfy themselves as to the expertise and experience of the outsourcing provider.
- 8.7.4 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.
- 8.7.5 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.
- 8.7.6 Outsourcing arrangements should be subject to periodic reviews. Periodic reporting thereon should be made to management and the Board.

- 8.7.7 The Board and Senior Management remain responsible in respect of functions or activities that are outsourced.
- 8.7.8 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.