



## **INSURANCE AND PENSIONS COMMISSION**

**Directive on Governance and Risk Management for  
Insurance Companies**

**February 2025**

## Contents

1.	Preamble.....	3
2.	Objectives .....	7
3.	Scope of Application .....	9
4.	System of Governance .....	10
5	Risk Management System.....	26
6	Control Functions .....	37
8	Compliance Function.....	43
9	Actuarial function.....	48
11	Outsourcing.....	59
12	Enforcement.....	66

# 1. Preamble

- 1.1. Pursuant of the Insurance and Pensions Commission’s mandate to protect the rights, benefits and other interests of policyholders in terms of section 5(a) of the Insurance Act [Chapter 24:07], the Commission hereby issues this directive on “Governance and Risk Management for insurers”.
- 1.2. This directive is issued in terms of section 6(c) of the Insurance Act [Chapter 24:07], as read with section 3 of Statutory Instrument 69 of 2020 which empowers the Commissioner to formulate standards and practices for the conduct of insurance business with which registered insurers may be required to comply.
- 1.3. The Commission reserves the right to exempt Microinsurers from complying with any of the provisions stated in this Directive.
- 1.4. This directive is meant to provide minimum guiding principles to ensure that insurers have effective systems of risk management including governance structures, internal controls and oversight functions.

## Interpretations

“Actuarial Function Report (AFR)” means a written report to be submitted to the board at least annually. The report shall document the tasks that undertaken by the Actuarial Function and their results.

“Appointed or Statutory Actuary” means a suitably qualified actuary appointed for statutory purposes following approval from IPEC who will apply a “fit and proper” test to such appointment.

“Board” means the board of directors.

“Close relative”, in relation to an individual, means any of the following persons-

- a. The individual’s grandparent, parent, brother, sister, child or grandchild, whether such relationship arises through blood or adoption;
- b. The individual’s step-grandparent, stepparent, step-brother, step-sister, step-child or step grandchild;
- c. Where the individual is married, his or her spouse or his or her spouse’s grandparent, parent, brother, sister, child or grandchild, whether such relationship arises through blood or adoption and the expression “closely related” shall be construed accordingly;

"Compliance risk" means the risk of undertaking legal responsibility, supervisory punishment, financial losses or reputation losses as a result of non-compliance by the insurance company or any of its employees and marketing staff.

"Control Function" within a system of governance, means the risk-management function, the compliance function, the internal audit function and the actuarial function.

"Credit risk" The risk of loss due to contractual obligations not being met (in terms of quantity, quality or timing) either in part or in full, whether due to inability of, or decision by, the counterparty. Credit risk comprises default and settlement risk. Credit risk can arise on issuers of securities (in the company's investment portfolio), debtors, or counterparties (e.g. on reinsurance contracts, or deposits) and intermediaries, to whom the company has an exposure. A related but different type of risk, classified under market risk is spread risk, which refers to the risk of a change in value due to movements in the market price of credit risk.

"Fit and proper criteria" for the purposes of these guidelines means the criteria that should be taken into account in determining whether one is suitable for appointment to a particular position and broadly include honesty, integrity, and reputation, competence and capacity; and financial soundness of the person to be so appointed. One shall be considered to have failed that test or criterion if the person has;

- a) been issued a warning or reprimand by the Commission, any other regulatory body, an operator of a market or clearing facility, any professional body or government agency.
- b) had any judgment (in particular; that associated with a finding of fraud, misrepresentation, financial mismanagement or dishonesty) entered against the relevant person in any civil proceedings. Where the applicant is a party to any pending proceedings which may lead to such a judgment, under any law in any jurisdiction, the Commission will hold the application in abeyance pending finalization of the said proceedings;
- c) been convicted of any offence of financial fraud. Where the applicant is a subject of any pending proceedings which may lead to such a conviction, under any law in any jurisdiction the Commission shall hold the application for appointment of the applicant in abeyance pending finalization of the said proceedings;
- d) been a director or a member of management of any financial institution in Zimbabwe that has become insolvent; or is facing insolvency proceedings due to financial mismanagement unless it is proven that the director or manager under question was not involved in the said mismanagement.

“Insurer” or “Underwriter” means a person, including a society, carrying on insurance business otherwise than as an insurance agent or as an insurance broker, who is not a person or a member of a class of persons declared to be exempt from the Insurance Act in terms of paragraph (c) of section two of the Act.

“IPEC” means the Insurance and Pensions Commission established in terms of the Insurance and Pension Commission Act [Chapter 24:21]

“Legal risk” – means the possibility that lawsuits, adverse judgements from courts, or contracts that turn out to disrupt or adversely affect the operations and/or financial condition of an insurer. The result may lead to unplanned additional payments or that contracts are settled on an unfavourable basis e.g. unrecoverable reinsurance.

“Liquidity risk” means the risk of failing to meet contractual obligations as and when they fall due. The risk may stem from the lack of marketability of an investment leading to the said investment or asset being disposed at a loss. Liquidity risk may arise due to illiquidity of the assets held to meet cash flow requirements (commonly referred to as asset, market, or trading liquidity risk), but also due to insufficient funds being available to meet cash flow requirements (funding liquidity risk).

“Market risk” means the risk of changes in values caused by market prices or volatilities of market prices differing from their expected values. It mainly arises from movement in equity prices, exchange rate, commodity prices or interest rates.

“Operational risk” The risk of a change in value caused by the fact that actual losses, incurred for inadequate or failed internal processes, people and systems, or from external events (including legal risk), differ from the expected losses.

“Principal Officer” means the Chief Executive Officer, Managing Director, General Manager or any other officer of the insurer responsible for the general control, direction and supervision of the insurer. The Principal Officer of the insurer shall be the highest authority reporting to the board of directors.

“Principle of proportionality” requires that the actions undertaken be proportionate to the size, nature, scale and complexity of the business of an insurance undertaking.

“Provisioning/Reserving risk” is the risk that insurance liabilities recorded by the insurer, net of reinsurance and other recoveries in respect of those liabilities, will be inadequate to meet the net amount payable when the insurance liabilities crystallise.

“Reinsurance risk” is the risk of inadequate reinsurance cover, which may be triggered by a situation such as the insolvency of a reinsurer, discovery of exposures without current reinsurance coverage, or exhaustion of reinsurance covers through multiple losses.

“Reputational risk” refers to the risk of adverse publicity emanating from an insurer’s business practices and associations, whether accurate or not, causing loss of confidence in the integrity of the institution. Reputational risk could arise from other risks inherent in an organisation’s activities.

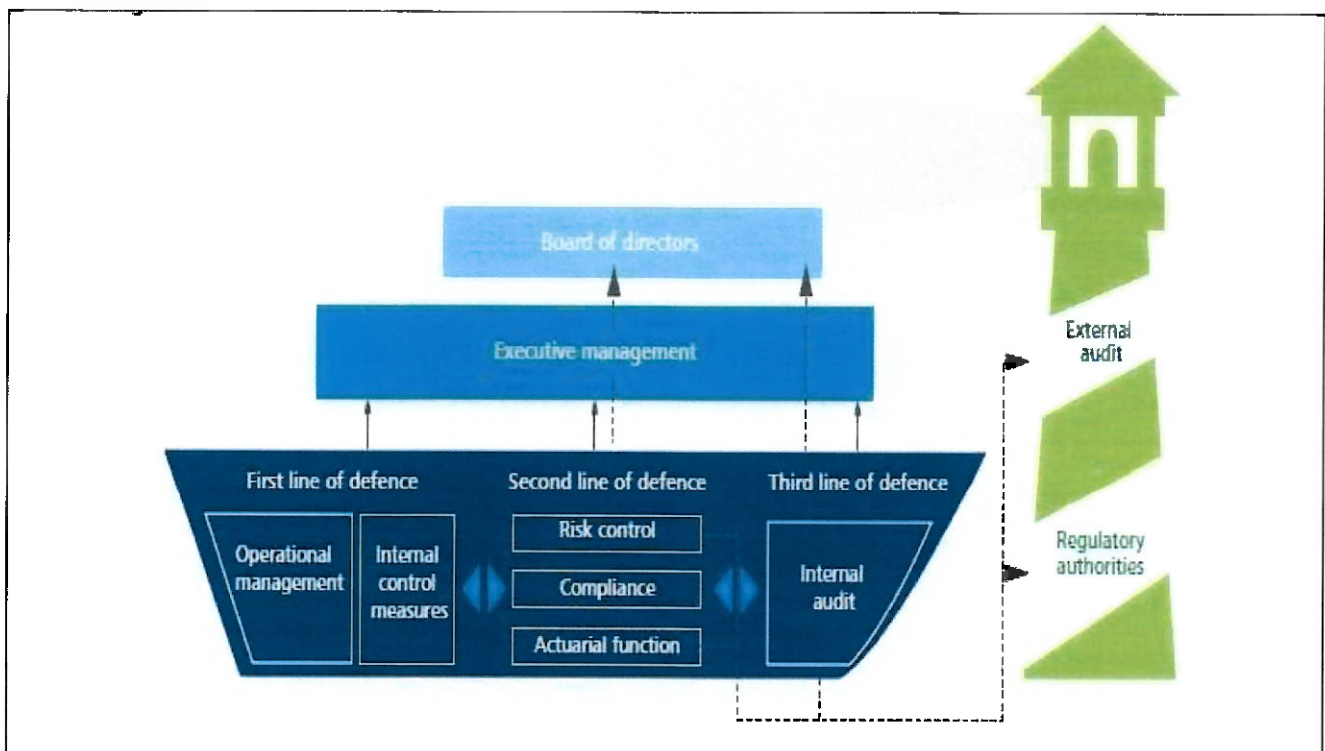
“The Act” in this framework refers to the Insurance Act [Chapter 24:07] or whichever act will govern insurance operations in Zimbabwe.

“Three lines of defence” model - this is a risk management model for financial institutions that distributes risk management responsibilities between stakeholders within an institution.

“Underwriting risk” The risk of a change in value due to a deviation of the actual claims payments from the expected amount of claims payments (including expenses). Total underwriting risk for non-life insurance includes the total of claims risk and expense risk for claims. For life insurance, it includes the total of lapse, surrender, and biometric risks, as well as expense risk for claims.

## 2. Objectives

- 2.1. The objective of this directive is to outline the minimum IPEC expectations and requirements for shareholders, board and management control functions of an insurer to ensure an effective governance and risk management framework is in place.
- 2.2. This directive is also meant to ensure that underwriters are managed in a sound and prudent manner by having in place systems for identifying, assessing, monitoring, and mitigating the risks that affect their ability to meet their obligations to policyholders. An insurer shall adopt sound and appropriate governance practices and procedures to support its work in a manner that promotes efficient, objective and independent judgment and decision-making.
- 2.3. The directive is based on the Three Lines of Defence model, which is emerging as the best practice standard for the positioning of key control functions within an underwriter. “Three Lines of Defence” Model
- 2.4. The three lines model below illustrates the different positioning of the different functions in an underwriter’s structure for effective governance.



Adopted: Positioning the Internal Audit Function within the solvency II framework; Ludovic Bardon et al...

- 2.5. As a first line of defence, operational management, has ownership, responsibility, and accountability for running the affairs of the underwriter, including designing and

implementing internal control measures, assessing, controlling, and mitigating the risks faced by an underwriter.

2.6. As a second line of defence, the risk management function facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in the management of all material risks. Compliance is responsible for ensuring implementation of the necessary procedures to comply with legal and other obligations, both internal and external to the insurer. The actuarial function provides assurance to the board of directors and management regarding the accuracy of the calculations and the appropriateness of the assumptions underlying the premiums, insurance liabilities and the capital adequacy requirements.

2.7. As a third line of defence, the Internal Audit Function will, through a risk-based approach, provide assurance to the underwriter's board and senior management, on how effective the underwriter assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an underwriter's risk, compliance, and actuarial management framework i.e. from risk identification, risk assessment and response to communication of risk related information (throughout the underwriter and to senior management and the board.)<sup>1</sup>

---

<sup>1</sup> Adopted from "The role of internal audit in solvency II" by a workgroup comprising of Hans Joachim Busselberg et al.

### 3. Scope of Application

- 3.1. This directive is applicable to all insurers registered to underwrite insurance business in the Republic of Zimbabwe.
- 3.2. This directive shall be used in conjunction with all other legislation pertaining to Insurance entities operating in Zimbabwe, including Circulars issued by IPEC.
- 3.3. This directive is a replaces the 2023 Directive on Governance and Risk Management for Insurance Companies issued under Circular 7 of 2023.
- 3.4. The Commission reserves the right to amend this directive from time to time.

## 4. System of Governance

### 4.1 Introduction

4.1.1. The system of corporate governance of an insurer should-

- a) promote the development, implementation and effective oversight of policies that clearly define and support the objectives of the insurer;
- b) define 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;
- c) set requirements relating to how decisions and actions are taken including documentation of significant or material decisions, along with their rationale;
- d) provide sound remuneration practices which promote the alignment of remuneration policies with the long-term interests of insurers to avoid excessive risk taking;
- e) provide for communicating with the Commission, as appropriate, matters relating to the management and oversight of the insurer; and
- f) provide for corrective actions to be taken for non-compliance or weak oversight, controls or management.

(Adopted from Insurance Core Principles).

### 4.2 Shareholding Structure

4.2.1 The term significant ownership and control over an insurer means-

- a) holding of issued shares or financial instruments (such as compulsory convertible debentures) above 10% of total issued shares or debentures in an insurer or its ultimate beneficial owner, or
- b) voting rights attached to the aforementioned shares i.e. more than 10% of issued shares or financial instruments, or
- c) power to appoint directors to the board and other executive committees or remove them.

4.2.2 No person shall acquire significant ownership or control in an insurance company without written approval by the Commission. The Commission shall issue such approval after conducting a fit and proper test.

4.2.3 In a bid to manage conflict of interest in placement of business, no insurer, shareholder of such an insurer, director or senior manager of an insurer, or such director/senior manager

and his or her close relatives shall, directly or indirectly hold significant ownership and control in the affairs of an insurance broker, or reinsurance company and vice versa unless with the written approval from the Commission which approval will be subject to provision 4.2.4 below.

4.2.4 Where an insurer has, in terms of section 4.2.3, received an approval from the Commission to own or hold significant ownership and control in the affairs of an insurance broker, or reinsurance company or vice versa, the exposure to an insurance broker in question or reinsurance company in terms of the business generated from the broker or placed with a reinsurer shall not exceed 20 per centum of the total business generated in terms of gross premium received.

4.2.5 No individual or such individual and his or her close relatives who have, directly or indirectly, significant ownership and control as defined in 4.2.1 shall be an employee or director of the insurer.

4.2.6 This position is meant to manage conflict of interest arising from failure to separate ownership from management which has in most instances prejudiced policyholders.

4.2.7 No nominee company or family trust shall, directly or indirectly, own significant shareholding in an insurance company unless the ultimate beneficial owners of such nominee company or the control information of the family trust has been revealed to the Commission and the trust should be registered.

#### 4.3 Composition and Governance of Board of Directors

##### 4.3.1 For purposes of this section-

A senior manager means an individual who directly reports to the Principal Officer of an insurance company.

A non-executive director means an individual who is not involved in the day-to-day management of the insurer or has not been so involved at any time during the past three (3) years; and

An independent director means a non-executive director who does not have any vested interests or conflict of interest deemed material by the Commission and includes a director who -

- a) is not and has not in the preceding five (5) years held an executive position within the insurer or any of its related persons;

- b) is not a close relative of an individual mentioned in subparagraph (a); or
- c) is not a material supplier or customer of the insurer or does not have any business relationship with the insurer, such that a reasonable and informed third party would conclude in the circumstances, that the integrity, impartiality or objectivity of that director is compromised by that relationship;
- d) is not associated to an adviser or consultant to the insurer or a significant customer or supplier of the insurer or with a not-for-profit entity that receives significant contributions from the insurer; or within the preceding five (5) years, has not had any business relationship with the insurer (other than service as a director); and
- e) is not employed by a public listed company at which an executive officer of the insurer serves as a director.

4.3.2 No director, senior manager or head of any control function shall be appointed by an insurer without written approval by the Commission. An application for such approval shall be made to the Commission with the necessary vetting documents to enable fit and proper assessment.

4.3.3(a) (i) The majority of the Board of Directors of an insurer shall at all times consist of nonexecutive directors. The majority of the Non-Executive Directors must be independent to promote objectivity in decision making by the board of Directors. The Principal Officer shall be an ex-officio member of the Board of Directors of the insurer.

(ii) The Board of Directors may invite any person to attend a meeting of the Board of Directors where the Board of Directors considers that the person has special knowledge or experience in a matter to be discussed by the Board of Directors at that meeting:

Provided that the invited person shall not have any voting rights.

(iii) The Independent Directors shall be free from any business relations or other associations, including those arising out of involvement in the past management or as a supplier, customer, or adviser that could materially interfere with the exercise of their independent judgment.

(iv) Where the Articles of Association of the insurer allows for the appointment of an alternate director, such appointment shall be approved by the Commission and the person so appointed shall not be a sitting member of the Board of Directors.

(b)(i) The Board of Directors of an insurer shall consist of an appropriate number and mix of individuals to ensure that there is an overall adequate spread and level of expertise at Board

level commensurate with the nature, scale and complexity of the business and risks of the insurer.

- (ii) The Board of Directors must at least have individuals with qualifications and or experience in insurance and risk management, investment, legal, accounting and ICT.
- (iii) Directors appointed based on professional skills are prohibited from offering their professional services to the insurer or reinsurer.

4.3.4 No non – executive director shall sit on the board of directors of the same insurance company for a tenure of more than two terms, provided that each term of office shall not exceed 5 years.

4.3.5 An employee or director of an insurance company shall not be an executive or a director of any other insurance company, reinsurance company or insurance broker and vice versa. Notwithstanding the foregoing, for holding companies the Group Chief Executive Officer may be allowed to sit on all the boards of the subsidiary companies.

4.3.6 In addition, to ensure that board members devote adequate time to the business of an insurance company in question, a director of such an insurance company shall not be a director for more than five companies including the insurance company in question.

4.3.7 Notwithstanding the above, directors of insurance companies within the same group are permitted to sit on the boards of all other such insurance companies.

4.3.8 To promote checks and balances, the chairperson of the board shall be an independent non-executive director and shall not serve as chairperson of any board committee.

4.3.9 While the board as a whole remains collectively responsible for the stewardship of the insurer, the board chairperson has the pivotal role of providing leadership to the board for its proper and effective functioning.

4.3.10 The role of the board chairperson encompasses responsibilities such as-

- a) setting the board's agenda,
- b) ensuring that there is adequate time allocated for the discussion of agenda items, especially if they involve strategic or policy decisions of significant importance,
- c) promoting a culture of openness and debate by facilitating effective participation of non-executive and management and communication between them and key persons in control functions,
- d) providing overall leadership to the board,

- e) ensuring proper induction, training and continuous development of board members,
- f) ensuring that the board is appropriately composed in compliance with the laws,
- g) ensuring that there is a formal and documented succession plan for the board,
- h) ensuring appropriate conduct of board meetings in accordance with the law, and
- i) ensuring that decision making process is in accordance with the law and that it caters for interests of the policyholders and shareholders.

4.3.11 In addition, to the appointment of the board chairperson, the board shall also appoint a lead independent director who shall also be the deputy chairperson of the board.

4.3.12 The functions of the lead independent director are to, amongst others,

- a) provide leadership and advice to the board of directors in respect of matters where the chairperson has actual or perceived conflict of interest, including by identifying circumstances where the chairperson may have actual or perceived conflict of interest that may impact on the chairperson's independent decision making;
- b) preside at meetings of the board of directors from which the chairperson is absent or in respect of which the chairperson has a conflict of interest or perceived conflict of interest; and
- c) perform the functions of the chairperson that cannot be performed by the latter because of a conflict of interest or perceived conflict of interest.

4.3.13 The board of directors of an insurer shall –

- a) have appropriate internal governance practices and procedures to support its work in a manner that promotes efficient, objective and independent judgment and decision making;
- b) have adequate powers and resources to discharge its duties fully and effectively;
- c) have systems and controls to ensure appropriate, timely and effective communications with the Commission on the governance of the insurer; and
- d) adopt and implement a procedure to conduct self-evaluation of the performance of the board as a whole and peer review of any director by other directors at least annually. In addition, the board shall be evaluated by an independent party at least once in every three years and documented results of such an evaluation shall be submitted to the Commission within 90 days after the completion of the evaluation.

#### 4.4 Board Charter

- 4.4.1 In addition to the articles and memorandum of association, every insurer is required to put in place a board charter.
- 4.4.2 The board charter shall document practices and procedures for the board's own internal governance, and the insurer shall ensure that these are followed and periodically reviewed to assess their effectiveness and adequacy.
- 4.4.3 The board charter shall set out how the board will carry out its roles and responsibilities. It shall 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 judgment.
- 4.4.4 Appropriate succession planning should also form part of the board's internal governance practices and should also be documented in the board charter.

#### 4.5 Fiduciary Duties of Directors

- 4.5.1 The directors shall individually and collectively-
- a) act in good faith, honestly and reasonably;
  - b) exercise due care and diligence;
  - c) act in the best interests of the insurer and policyholders, putting those interests ahead of his/her own interests;
  - d) exercise independent judgment and objectivity in his/her decision making, taking due account of the interests of the insurer and policyholders;
  - e) not use his/her position to gain undue personal advantage or cause any detriment to the insurer; and
  - f) at all times comply with the fit and proper policy of the insurer.

#### 4.6 Roles and Responsibilities of Board of Directors

- 4.6.1 The board of directors is responsible for the effective governance and risk management of an insurer.
- 4.6.2 The board of directors of an insurer shall –
- a) determine and oversee the implementation of the insurer's corporate culture, business objectives and strategies for achieving those objectives, which objectives and strategies

shall be regularly reviewed to be consistent with the long-term interests and sustainability of the insurer and the interests of its policyholders;

- b) ensure that the roles and responsibilities allocated to the board of directors, senior management and heads of control functions are clearly defined so as to promote an appropriate separation of oversight function from management responsibilities;
- c) ensure that there are adequate policies and procedures relating to the appointment, dismissal and succession of senior management and heads of control functions;
- d) develop a formal, documented process for nomination, selection, and removal of the board members;
- e) provide oversight in respect of senior management and the design and implementation of sound risk management and internal control systems;
- f) adopt, oversee and enforce the effective implementation of all policies of the insurer, including, but not limited to-
  - i. the overall risk management policy and component policies; and
  - ii. a written remuneration policy for the insurer, which does not induce excessive or inappropriate risk taking, and shall be in line with the corporate culture, objectives, strategies, identified risk appetite, and long term interests of the insurer, and has proper regard to the interests of its policyholders and other stakeholders. The board shall also ensure that such a remuneration policy, at a minimum, covers 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.
- g) monitor compliance with the Insurance Act and other applicable laws as well as its fit and proper policy to facilitate the sound and prudent management of the business of the insurer;
- h) ensure that systems and controls are in place to ensure the promotion of appropriate, timely and effective communication with the Commission on the governance framework of the insurer, which will allow the latter to make informed judgments about the effectiveness of the board of directors and senior management in governing the insurer;
- i) make sure that the insurer has adequate policies and procedures governing the appointment and removal of the principal officer;
- j) have appropriate policies and procedures to ensure that senior management –

- i. carry out the day-to-day operations of the insurer effectively and in accordance with the insurer's strategies, policies and procedures;
- ii. promote a culture of sound risk management, compliance and policyholder protection;
- iii. provide the board of directors with adequate and timely information to enable it to carry out its duties and functions, including the monitoring and review of the performance and risk exposures of the insurer, and the performance of senior management; and
- iv. provide the Commission and relevant stakeholders with the information required to satisfy the legal and other obligations applicable to the insurer;
  - k) regularly monitor and evaluate the adequacy and effectiveness of the insurer's governance framework and notify the Commission of any shortcomings and the reasons thereof;
  - l) ensure there is a reliable financial reporting process for both public and IPEC purposes that is supported by clearly defined roles and responsibilities of the board, senior management and the external auditor;
  - m) ensure fair treatment of the shareholders, policy holders and employees; and
  - n) ensure that there is adequate governance and oversight of the external audit process.

4.6.3 The board of directors of an insurer shall develop an appropriate system of delegation, which delegation shall -

- a) be appropriately and clearly mandated;
- b) provide adequate checks and balances;
- c) provide for the monitoring and reporting on delegations;
- d) not allow for the undue concentration of powers; and
- e) provide for the withdrawal of a delegated responsibility.

4.6.4 Anything done or omitted to be done under a delegation –

- a) does not in any way abrogate the accountability of the board of directors; and
- b) is deemed to have been done or omitted by the board of directors.

#### 4.7 Meetings for the Board of Directors

4.7.1 The board of directors of an insurer shall meet at least once every quarter.

4.7.2 The quorum of the board of directors shall be three fifths of the directors provided that the majority of the quorum shall not be executive directors and the same majority shall be made up of independent directors.

4.7.3 Decisions of the board and/or its committee shall be recorded in writing and shall be made by a majority of votes. Where an individual director feels strongly about any issues but fails to garner enough votes to form a board resolution, he/she shall request his/her position to be put on record.

4.7.4 This may help to exonerate individual directors where the board will have collectively made decisions that prejudiced policyholders, leading to regulatory action being taken on directors by IPEC.

#### 4.8 Committees of the Board

4.8.1 At a minimum, the board shall have the following committees:

- a) Risk Management Committee;
- b) Nomination and Remuneration Committee; and
- c) Audit Committee; and
- d) Finance Committee

4.8.2 Committees of the board shall –

- a) be structured to ensure that they have the necessary authority, independence, resources and expertise.
- b) have documented terms of References or Charters which will address among other things, the mandates, functions, composition, qualifications, duties etc of the same committees; and
- c) have access to all relevant employees, independent professional advice and information to perform their mandate and functions.

#### 4.9 Risk Management Committee

4.9.1 A risk management committee shall comprise at least three members who do not necessarily need to be board members. Where members of this Committee are not directors of the

company, their appointment shall be subject to approval by the Commission which shall apply fit and proper person criteria.

4.9.2 The chairperson of the risk management committee shall be an independent director with expertise in risk management.

4.9.3 The committee shall meet at least once quarterly.

4.9.4 A risk management committee shall perform the following functions-

- a) deal with all actuarial matters if no other committee is designated to deal with the same issues;
- b) assist the board of directors in its evaluation of the adequacy and effectiveness of the risk management system;
- c) assist the board of directors in identifying and regularly monitoring all material risks to ensure that its decision-making capability and accuracy of its reporting is maintained;
- d) facilitate and promote communication, through reporting structures, regarding the matters in respect of risk management or any other related matter, between the board of directors and senior management;
- e) ensure the establishment of an independent risk management function;
- f) introduce such measures as may serve to enhance the adequacy and effectiveness of the risk management system;
- g) co-ordinate the monitoring of risk management on an enterprise-wide and individual business unit basis; and
- h) mandated to deal with all reinsurance matters as well as any other alternative risk transfer matters.

#### 4.10 Nomination and Remuneration Committee

4.10.1 A remuneration committee shall consist of at least three members who shall be nonexecutive directors or any other members who may not be directors of the company. Where members of this Committee are not directors of the company, their appointment shall be subject to approval by the Commission which shall apply fit and proper person criteria.

4.10.2 The chairperson of the nomination and remuneration committee shall be an independent director.

4.10.3 The principal officer shall be prohibited from being a member of the nomination and remuneration committee.

4.10.4 The nomination and remuneration committee shall meet at least once quarterly.

4.10.5 A nomination and remuneration committee shall perform the following functions-

- a) develop an appropriate remuneration policy referred to in section 5.4;
- b) monitor the implementation of an insurer's remuneration policy and regularly review the suitability of that policy;
- c) undertaking due diligence enquiry in respect of directors and senior management with a view to ensure that the directors and senior management of the insurer meet the "fit and proper" criteria after every 5 years. The criteria to be satisfied, at a minimum, would relate to integrity demonstrated in personal behaviour and business conduct, soundness of judgment and financial soundness.

The nomination and remuneration committee shall scrutinize the declarations of the applicants before the appointment or reappointment or election of directors by the shareholders at annual general meetings. The nomination and remuneration committee shall also make independent or discreet references, where necessary, well in time to verify the accuracy of the information furnished by the director.

The insurers are further required to obtain an annual declaration from the directors that the information provided in the declaration at the time of appointment or reappointment has not undergone any change subsequently and the changes, if any, are appraised by the concerned director to the board; and

- d) discuss all human resources issues relating to the insurer.

#### 4.11 Audit Committee

4.11.1 Every registered insurer shall appoint an audit committee consisting of-

- a) a chairperson, who shall be an independent director with a strong finance and accounting background; and
- b) at least two other independent non-executive directors.

4.11.2 The head of the Internal Audit functions attends the Audit Committee by invitation at allocated times and shall have deliberative but not voting rights.

4.11.3 The principal officer of the insurance company shall be prohibited from sitting on the audit committee except if he is sitting by invitation only for the purposes of eliciting any specific information concerning audit findings.

4.11.4 The functions of an audit committee shall be to-

- a) establish appropriate accounting policies and practices and controls in respect of the business for the insurer;
- b) assisting the insurer's board to evaluate the adequacy and efficiency of the internal control systems, accounting practices, information systems and auditing processes applied in the day-to-day management of the insurance business and put in place remedial action;
- c) overseeing the financial statements, financial reporting and disclosure processes as well as introducing such measures as, in the audit committee's opinion, may enhance the objectivity of financial statements and reports prepared with reference to the business of insurer;
- d) overseeing the internal audit process (reviews by internal audit of the insurer's financial reporting controls) and reviewing the internal auditor's plans and material findings;
- e) reporting to the Commission on significant issues concerning the financial reporting process, including actions taken to address or mitigate identified financial reporting risks; and
- f) selecting a suitably-qualified person for appointment as the head of internal audit and external auditors of the insurer subject to approval by the Commission.

4.11.5 An external audit firm shall serve an insurer for a maximum of five years after which he can only serve as an external auditor for the same insurer after serving a cooling off period of three (3) years. The external auditor shall pay due regard to the fact that an insurance entity is a public entity when conducting his duties.

4.11.6 External auditors shall be required to seek the advice of qualified actuaries and other professionals where they do not have sufficient in-house expertise on actuarial issues.

4.11.7 External auditors shall also be obliged to advise the Commission where within thirty (30) days after identifying issues of regulatory concern that may threaten policyholder interests or the solvency of the insurance company.

4.11.8 Where the Commission requests access to documents obtained from the regulated entity in question or any other document obtained from any other source that was used in formulating the external auditor's opinion or generating the auditor's report, the same external auditor shall be required to comply with such requests.

4.11.9 An audit committee shall meet at least once quarterly to carry out its functions.

4.11.10 Decisions of an audit committee shall be decided by a majority vote of the members present, provided that no member shall abstain from any vote to be taken.

#### 4.12 Finance Committee

4.12.1 The Finance Committee shall be comprised of at least three directors. Where members of this committee are not directors of the company, their appointment shall be subject to approval by the Commission after conducting the fit and proper test.

4.12.2 The Chairperson of the Finance Committee shall be an independent director with the requisite qualifications and experience in Finance.

4.12.3 The Finance Committee shall meet at least once quarterly.

4.12.4 The functions of the Finance Committee shall include –

a) Monitoring the company's financial resources through reviewing its capital structure and annual capital plan, including assessment of capital adequacy and capital planning process, stress testing and related activities, capital raising, capital distributions as well as to approve and recommend to the board approval of annual capital plan submission and capital management policy.

b) To provide input into the crafting of the company's budgets and implementation.

c) Review financial aspects of the company's recovery and resolution plans.

d) Review any additional financial matters that the board may direct to the Committee.

#### 4.13 Policyholders' Protection Functions

4.13.1 The board shall ensure that the insurer develops a mechanism of keeping the policyholders well informed and educated about insurance products, claims and complaint-handling procedures and in particular shall.

- a) Put in place proper procedures and effective mechanism to address complaints and grievances of policyholders;
- b) Ensure compliance with the statutory requirements as laid down in the regulatory framework;
- c) Ensure adequacy of disclosure of “material information” to the policyholders; and
- d) Provide the details of grievances at quarterly intervals in such formats as may be prescribed by the Commission.

#### 4.14 Ethics Functions

4.14.1 The board’s responsibilities in respect to the ethics functions shall include ensuring that the insurer has mechanisms to enable:

- a) Supervising and monitoring matters reported using the insurer’s whistle blowing or other confidential mechanisms for employees and others to report ethical and compliance concerns or potential breaches or violations.
- b) Approval compliance programmes, reviewing their effectiveness on a regular basis and signing off on any material compliance issues or matters.

#### 4.15 Organisational Structures

4.15.1 The insurer shall establish a transparent organisational structure which supports the strategic objectives and operations of the insurer.

4.15.2 The structure shall be up to date, have clear reporting lines and cover all functions including those which are outsourced.

4.15.3 The board and senior management shall know and understand the structure and the risks that it poses.

#### 4.16 Duties of Senior Management

4.16.1 Senior management of the insurer is required to-

- a) carry out the day-to-day operations of the insurer effectively and in accordance with the insurer’s corporate culture, business objectives and strategies for achieving those objectives in line with the insurer's long-term interests and viability;
- b) promote sound risk management, compliance and fair treatment of customers;

- c) provide 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 senior management; and
- d) maintains all the records of the insurer relating to all running policies or policies where the insurer has not fully discharged their obligations, in an easily accessible manner. Where the insurer in question has discharged its obligations in respect of an insurance policy the insurer shall maintain all the records in respect of that policy for ten (10) years.

#### 4.17 Principal Officer, and Senior Management Major Duties and Responsibilities of the Principal Officer...

4.17.1 The principal officer shall be responsible to the board for the day to day running of the insurer. The principal officer shall;

- a) Ensure that the policies spelt out by the board in the insurer's overall corporate strategy of the institution shall be implemented;
- b) Through designed criteria and in adherence to the institution's human resources policy, identify and recruit competent officers. In the case of all key personnel and heads of control functions the Principal Officer shall identify and recommend to the board competent officers. Notwithstanding the foregoing, the Principal Officer shall however, be precluded from being involved in the appointment of Head of the Internal Audit Functions;
- c) Co-ordinate the operation of the various departments within the institution;
- d) Establish and maintain efficient and adequate internal control systems;
- e) Design and manage the necessary management information system in order to facilitate efficient and effective communication within the institution;
- f) Ensure that the board is frequently appraised about the operation of the institution through presentation of relevant board papers, which shall cover, but not limited to the following areas;
  - i. Actual performance and variance with the past and/or projected performance and the budget together with the explanation of the likely cause of all the variances.
  - ii. Capital structure and adequacy.

- iii. Income and expenditures. iv. Performance in terms of, investments, losses, recoveries and provisions.
- v. Reports on compliance with applicable laws, and directives issued by the Commission, and any violations to those laws, if any, and the remedial actions taken on such violation.
- vi. Large exposures. vii. Any other areas relevant to the Institution's operations.

Appointment of the Principal Officer and Senior Management to be Approved by the Commission...

- 4.17.2 No individual shall be appointed as a principal officer, head of a control function, Chief Finance Officer (or whatever title they may be called), Chief Operations Officer (or whatever title they may be called) or in any other senior management position of an insurer without written approval from the Commission.
- 4.17.3 The insurer shall apply to the Commission for approval of persons appointed in positions mentioned in 4.17.2 above. The insurers proposing such appointment shall provide the Commission with the necessary vetting documents to enable conduct of fit and proper assessment.
- 4.17.4 A principal officer shall be an individual who holds a minimum qualification of a diploma in insurance or an equivalent qualification from a recognised institution, or any other such qualification deemed appropriate, with at least five (5) years' experience in any senior position in any role within the insurance sector.
- 4.17.5 The Commission shall retain the power to disqualify any principal officer if it gathers any information about the principal officer that renders the Principal Officer not fit and proper or adversely affects the interests of policyholders. In such a case the Commission shall call upon the insurer to present another name for approval.
- 4.17.6 In case of the principal officer being out of office for a period of at least three (3) weeks the Commission shall be promptly informed of the development and the acting arrangements.

## 5 Risk Management System

### 5.1 Requirements for an Effective Risk Management System

5.1.1. An insurer shall establish and maintain an effective risk management system, comprising strategies, policies and procedures for identifying, assessing, monitoring, managing, and reporting of all reasonably foreseeable current and emerging material risks to which the insurer may be exposed.

5.1.2. The risk management system shall –

- a) adequately support the board of directors in meeting its responsibilities with respect to the furtherance of the safe and sound operation of the insurer and the protection of policyholders, taking into account the nature, scale and complexity of the insurer's business and risks;
- b) address risks on an enterprise-wide and individual business unit basis; and
- c) be embedded within the organisation, in particular in the key operations and structures of the insurer.

5.1.3. The risk management system shall, at least, include –

- a) a clearly defined relevant and well documented risk management strategy which takes into account the insurer's overall business strategy (as approved by the board of directors) and its business activities (including any business activities which have been outsourced);
- b) documented procedures which clearly define the decision-making processes within the framework of the risk management system;
- c) an adequate written overall risk management policy consistent with the risk management strategy;
- d) appropriate processes, procedures and tools (including, where appropriate, models) for identifying, assessing, monitoring, managing, and reporting (including communication and escalation mechanisms) on each material risk;
- e) report (regular and ad hoc) to inform senior management and the board of directors on the risk profile of the insurer, including each material risk faced by the insurer and on the effectiveness of the risk management system itself; and

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

5.1.4. The risk management system shall be reviewed regularly by the internal audit function or an objective, independent and qualified external party of the insurer to ensure that the system is effective and that necessary modifications are identified and made in a timely manner.

5.1.5. The risk management system and any modifications shall be documented and approved by the board of directors.

## 5.2 Overall Risk Management Policy

5.2.6. An insurer shall develop and regularly review an adequate written overall risk management policy that includes –

- a) a definition and categorisation of all reasonably foreseeable current and emerging material risks (including external and internal business specific, enterprise-wide and individual business unit risks) to which the insurer is exposed, taking into account the nature, scale and complexity of the insurer and its business;
- b) the approach of the insurer to assessing the materiality of the risks;
- c) the approach relating to the identification, assessment, monitoring, management and reporting of each risk, including assignment of specific risk management responsibilities across the insurer; and

5.2.7. The risk management framework shall at least, include the following -

- a) a fit and proper policy;
- b) A remuneration policy;
- c) a policy on management of underwriting risk, reinsurance and other forms of risk transfer, an investment policy, market risk, asset-liability management, liquidity risk management, operational risk management, insurance fraud risk management, credit risk management, reputational risk management, legal and compliance risk, concentration risk management.

### 5.3 Fit and Proper Policy

#### 5.3.1 An insurer's fit and proper policy shall, at least, -

- a) provide for the prudent management of the risks that a director, principal officer, senior management, public officer, auditor, statutory actuary (or his or her alternate), head of a control function or significant owner (collectively referred to as "responsible person") who is not fit and proper poses to its insurance business, financial soundness and fair treatment of policyholders;
- b) clearly define and document the fit and proper criteria required for each responsible person having regard to-
  - i) any prescribed fit and proper requirements; and
  - ii) the need to set high internal standards of ethics and integrity that promote sound corporate governance and appropriate and pertinent expertise, educational qualifications or experience, skills and knowledge in respect of the duties that such a person shall perform;
- c) include the processes (including the decision-making processes) to be undertaken in assessing whether a responsible person is fit and proper;
- d) specify the actions to be taken where the insurer assesses a responsible person as not being fit and proper, which shall include notifying the Commission of such an assessment and the actions taken;
- e) require periodic (at least annual) fit and proper assessments for each responsible person;
- f) require that sufficient documentation for each fit and proper assessment is retained to demonstrate the fitness and propriety of responsible persons and their immediate predecessors;
- g) provide that responsible persons consent to being subject to the fit and proper policy. Where the responsible person refuses to be subjected to fit and proper policy, they shall not be eligible for appointment or shall not continue to occupy the position for which the fit and proper assessment applies;
- h) include adequate provisions to allow confidential reporting if a person believes that a responsible person does not meet the insurer's fit and proper criteria and for the protection of such a person; and

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

#### 5.4 Remuneration Policy

5.4.1 This remuneration policy shall cover at least the following-

- a) board fees and sitting allowances;
- b) salaries for senior management and heads of control functions,
- c) the specific terms of performance-related plans including any profit-sharing arrangements, stock compensation, stock options, or other deferred-benefit compensation,
- d) pension plans,
- e) fringe benefits such as non-salary perquisites,
- f) termination policies including any severance payment policies; and
- g) Policy guidelines to be used for determining remuneration in individual cases, including specific criteria to be used in evaluating an officer's performance.

5.4.2 Although this directive is meant to ensure that insurer's remuneration strategies promote the viability of the insurer and protect interests of its policyholders, it is not 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.

5.4.3 In order to satisfy itself about the effectiveness of the remuneration policy and practices, the board shall consider at least-

- a) the components of the overall remuneration policy, particularly the use and balance of fixed and variable components;
- b) the performance criteria and their application for the purposes of determining remuneration payments;
- c) the remuneration of the members of the board, senior management and major risk taking staff; and
- d) any reports or disclosures on the insurer's remuneration practices provided to the Commission in a manner that may be prescribed from time to time or the public.

5.4.4 The board shall also ensure that the 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.

5.4.5 The potential for conflicts of interests that may compromise the integrity and objectivity of the staff involved in control functions shall be mitigated. This can be achieved by a variety of means, such as making their remuneration -

- a) predominantly based on the effective achievement of the objectives appropriate to such control functions;
- b) not linked to the performance of any business units which are subject to their control or oversight; and
- c) 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.

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

5.4.7 An insurer's remuneration policy shall -

- a) not induce excessive or inappropriate risk taking and be consistent with the long-term interests of the insurer and the interests of its policyholders;
- b) at a minimum, address the remuneration of directors, senior management, heads of control functions and other persons whose actions may have a material impact on the risk exposure of the insurer (including persons to whom functions are outsourced);
- c) be consistent with the insurer's business and risk management strategy (including the insurer's risk management practices), and performance;
- d) apply to the insurer as a whole in a proportionate and risk-based way and contain specific arrangements that take into account the respective roles of persons;
- e) provide for a clear, transparent and effective governance structure around remuneration, and the oversight of the policy;
- f) when remuneration includes both fixed and variable components, it shall provide that

- i. the fixed portion represents a sufficiently high portion of the total remuneration to avoid over dependence on the variable components;
  - ii. the variable component is based on a combination of the assessment of the individual and the collective performance, such as the performance of the business area and the overall results of the insurer;
  - iii. Guaranteed variable remuneration shall generally not be offered, as they are not consistent with sound risk management and performance-based rewards. iv. the payment of the major part of a significant bonus, irrespective of the form in which it is to be paid, contains a flexible, deferred component that considers the nature and time horizon of the insurer's business; and
  - iv. The award of variable remuneration shall contain provisions that enable the insurer, under certain circumstances, to apply 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 when risks of such performance have manifested after the award of variable remuneration;
- g) ensure that in defining an individual's performance, that financial and non-financial performance are considered.

5.4.8 The non-executive directors shall only be entitled to sitting allowances that are clearly defined within the remuneration policy and in line with their defined duties.

5.4.9 Executive directors shall not be entitled to any board sitting allowances in respect of their participation on the main board or board committees.

5.4.10 Clear provisions shall therefore be outlined governing relationships between nonexecutive directors and management. This shall cover aspects such as non-executive directors' access to other benefits from management such as holiday allowances, company cars among other benefits.

5.4.11 Where an insurer provides discretionary pay-outs on termination of employment, such payment shall be subject to appropriate governance controls and limits. In any case, such payouts shall be aligned with the insurer's overall financial condition and performance over an appropriate time horizon.

5.4.12 Severance payments shall be related to performance over time; shall not reward failure and shall 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.

## 5.5 Asset-Liability Management Policy

5.5.1 An insurer's asset-liability management policy shall -

- a) clearly specify the nature, role and extent of the insurer's asset-liability management activities and their relationship with product development, pricing functions and investment management;
- b) co-ordinate the management of risks associated with assets and liabilities and the complexity of those risks;
- c) recognise the interdependence between the insurer's assets and liabilities and take into account the correlation of risk between different asset classes and the correlations between different products and business lines; and
- d) take into account any off-balance sheet exposures that the insurer may have and the contingency that risks transferred may revert to the insurer.

## 5.6 Investment Policy

5.6.1 An insurer's investment policy shall-

- a) provide for the investment of all the insurer's assets in accordance with the Act;
- b) specify the nature, role and extent of the insurer's investment activities and how the insurer ensures compliance with the value of and limitations on assets requirements as prescribed under the Act;
- c) set out the insurer's strategy for investment activities and specify asset allocation strategies, how these will be managed and how these are related to the asset liability management policy;
- d) establish explicit risk management procedures with regard to more complex and less transparent classes of asset and investment in markets or instruments that are subject to less governance or regulation;
- e) take into account any factor which may materially affect the sustainable long-term performance of assets, availability of the assets and considered riskiness of the same, including factors of an environmental, social and governance character; and
- f) adhere to the 'Prudent Person Principle' by establishing measures that will assist in ensuring that -

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

5.6.2 An insurer's investment policy shall provide for -

- a) the investment of all assets, specifically those assets covering the financial soundness requirements, for investment in a manner that ensures the security, quality, liquidity and profitability of its whole portfolio of assets and the availability of assets;
- b) a conflict of interest, that investments are made in the best interest of policyholders and beneficiaries;
- c) assets held in respect of long-term policies where the investment risk is borne by the policyholders, that the liabilities -
  - i. in the case of policy benefits that are directly linked to the value of units, be represented as closely as possible by those units;
  - ii. in the case of policy benefits that are directly linked to a share index or a reference value other than units, be represented as closely as possible by the units deemed to represent the reference value or, in the case where units are not established, by assets of appropriate security and marketability which correspond as closely as possible with those on which the particular reference value is based;
- d) benefits referred to under c) above that include a guarantee of investment performance or another guaranteed benefit, for assets held to cover the corresponding additional liabilities to adhere to subsection 5.6.1 (f) (ii); and
- e) the proper diversification of assets in a manner that avoids excessive reliance on any particular asset, issuer or group of companies, or geographical area and excessive concentration of risk in the portfolio as a whole, for assets other than those referred to under c) above.

## 5.7 Liquidity Risk Management Policy

5.7.1 The liquidity risk management policy shall set out the approach to the identification, assessment, monitoring, management and reporting of short-term and long-term liquidity risk in order to meet the insurer's obligations as they fall due.

## 5.8 Underwriting Risk Management Policy

5.8.1 The underwriting risk management policy -

- a) identify the nature of the insurer's insurance business, including, but not limited to-
  - i. the classes of insurance to be underwritten; and
  - ii. the types of risks that may be underwritten and those that are to be excluded;
- b) describe the formal risk assessment process in underwriting, including, but not limited to-
  - i. the criteria used for risk assessment; ii. the method(s) for monitoring emerging experience; and
  - iii. the method(s) by which the emerging experience is taken into consideration in the underwriting process;
- c) set out the actions to be taken by the insurer to assess and manage the risk of loss, or of adverse change in the values of insurance and reinsurance liabilities, resulting from inadequate pricing and provisioning assumptions;
  - i. set out the relevant data (quantity and quality) to be considered in the underwriting and reserving processes; and
  - ii. provide for the regular review of the adequacy of claims management procedures, including the extent to which they cover the overall cycle of claims.

## 5.9 Reinsurance and Other Forms of Risk Transfer Policy

### 5.9.1 An insurer's reinsurance and other forms of risk transfer policy -

- a) outline appropriate strategies and procedures for the selection of suitable reinsurance programs and other risk transfer techniques, proportionate to the nature, scale and complexity of the insurer's risks, and to the capabilities of the insurer to manage and control the risk transfer technique used;
- b) ensure transparent reinsurance arrangements that enable the Commission to understand the economic impact of reinsurance and other forms of risk transfer arrangements in place;
- c) provide for processes and procedures for ensuring that the strategies referred to in paragraph a) above are implemented and complied with, and that the insurer has in place appropriate systems and controls over its risk transfer transactions;
- d) identify the level of risk transfer appropriate to the insurer's approach to risk;

- e) identify the types of reinsurance arrangements most appropriate to effectively manage the insurer's risk profile;
- f) identify principles for the selection of reinsurance counterparties;
- g) provide for procedures for assessing the creditworthiness and diversification of reinsurance counterparties;
- h) provide for procedures for assessing the effectiveness of the risk transfer;
- i) set concentration limits for credit risk exposure to reinsurance counterparties and appropriate systems for monitoring these exposures; and
- j) provide for liquidity management to address any timing mismatch between claims payments and reinsurance recoveries.

#### 5.10 Concentration Risk Management Policy

5.10.1 The concentration risk management policy shall set out the approach to be taken to -

- a) identify relevant sources of concentration risk to ensure that risk concentrations remain within established limits; and
- b) analyse possible risks of contagion between concentrated exposures.

#### 5.11 Operational Risk Management Policy

5.11.1 The operational risk management policy shall set out the approach to the identification, assessment, monitoring, management and reporting of relevant operational risk exposures (including the risks associated with inadequate or failed internal processes, people or systems, or from external events).

5.11.2 The operational risk management policy shall make provision for-

- a) A business continuity plan;
- b) A disaster recovery site;
- c) Training of personnel; and
- d) Data integrity and Backup of data.

5.11.3 As part of operational risk management, an insurer shall establish, maintain and operate within an adequate and effective internal control system, comprising strategies, policies, procedures and controls to provide the board of directors and senior management with

reasonable assurance from a control perspective that the insurance business is operated consistently with –

- a) the strategy determined by the board of directors;
- b) the business objectives of the insurer;
- c) the key business, information technology, financial policies and processes, and related risk management policies and procedures, determined by the board of directors; and
- d) the legislation that applies to the insurer.

5.11.4 The internal control system shall be appropriate to the nature, scale and complexity of the insurer's business and risks and shall, at least, provide for –

- a) appropriate controls to provide reasonable assurance over the fairness, accuracy, and completeness of the insurer's financial and non-financial information;
- b) appropriate segregation of duties, and controls to ensure that such segregation is observed;
- c) appropriate controls for other key business procedures and policies;
- d) a delegation of authority, approved by the board of directors, regularly reviewed by the board of directors;
- e) controls at the appropriate levels so as to be effective, including at the procedure or transactional level, and at the legal entity or business area level;
- f) regular monitoring of all controls to ensure that -
  - i. The controls form an integrated system; and
  - ii. The internal control system -
    - functions as intended;
    - fits within the overall governance framework; and
    - complements the risk identification, risk assessment, and risk management activities of the insurer;
- g) regular independent testing and assessments (carried out by objective parties such as an internal or external auditor) to determine the adequacy, completeness and effectiveness of the internal control system;

- h) a written inventory of key procedures and policies insurer-wide, and of the controls in place in respect of such procedures and policies; and
- i) training in respect of relevant components of the internal control system, particularly for employees in positions of trust or responsibility, or carrying out activities that have significant risk.

5.11.5 The operational risk management policy shall also have provisions relating to

Insurance Fraud Risk Management. These provisions shall –

- a) outline appropriate strategies, procedures and controls to deter, prevent, detect, report and remedy insurance fraud, and to effectively manage fraud risk and possible risks to the insurer's financial soundness or sustainability caused by fraud; b) take into consideration how the effectiveness of fraud risk management may be enhanced through contributing towards industry-wide initiatives to deter, prevent, detect, report and remedy insurance fraud; and
- c) provide for the reporting of insurance fraud to relevant regulatory authorities within two (2) days after becoming aware of the fraud or potential fraud.

## 6 Control Functions

### 6.1 General Requirements for Control Functions

6.1.1 An insurer shall establish and maintain the following control functions-

- a) Risk management function;
- b) Compliance function;
- c) Internal Audit function; and
- d) Actuarial function

6.1.2 An insurer, in light of its nature, scale and complexity of the business risks, legal and regulatory obligations, may opt to outsource a control function subject to the Commission's approval.

6.1.3 The Commission may exempt an insurer from the requirement to establish and maintain an actuarial function if the Commission is of the opinion that it is appropriate given the nature, scale and complexity of the insurer's business and risks.

6.1.4 Each control function shall be structured such that the function has the necessary authority, independence, resources, expertise and access to the board of directors or a committee of the board identified by the board of directors and all relevant employees and information to exercise its authority and perform its responsibilities. Pursuant of the need for the control functions to have the necessary authority, the heads of control functions shall be placed at the same level as other Key Managers in the insurance company.

6.1.5 The independence be sufficient to allow a control function to -

- a) serve as a further component of an insurer's checks and balances;
- b) provide an objective perspective on strategies, issues, and potential non-compliance related to its areas of responsibility; and
- c) implement or oversee the implementation of corrective measures where necessary.

6.1.6 The authority and responsibilities of each control function be determined and documented under the governance framework of the insurer referred.

6.1.7 The insurer's internal audit function or an objective and independent and qualified external reviewer regularly review the risk management function, compliance function and actuarial function.

6.1.8 An independent and objective external reviewer shall review the internal audit function after every three (3) years.

6.1.9 The board of directors shall regularly review the performance of each control function, taking into consideration the reviews referred to under paragraphs (6.1.6) and (6.1.7).

6.1.10 The existence of any control function does not relieve the board of directors or senior management of their respective governance and related responsibilities.

6.1.11 Each control function shall -

- a) avoid conflicts of interest, and if any conflict cannot be avoided, report that conflict to senior management and the board of directors; and
- b) comply with the requirements relating to the reporting structures, independence, resources, expertise, responsibilities and functions referred to in sections 7 to 9.

Function

6.2.1 An insurer shall appoint a head for each of the control functions.

6.2.2 The appointment, performance assessment, remuneration, disciplining and dismissal of the head of each control function (other than the head of the internal audit function) shall be

done with the approval of, or after consultation with, the board of directors or relevant board committee.

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

6.2.4 An insurer may, where appropriate in light of the nature, scale and complexity of the insurer's business and risks, appoint -

- a) a person as the head of more than one control function (other than the head of the internal audit function); or
- b) subject to the approval of the Commission, the statutory actuary as the head of the actuarial function, if that appointment provides that the statutory actuary may not conduct any activities for the insurer which would compromise the independence and oversight requirements of the role of the actuarial function.

6.2.5 An insurer shall not outsource the head of control function in respect of the risk management function, actuarial, compliance function and internal audit function without the approval of the Commission.

6.2.6 The head of each control function shall -

- a) regularly report to the board of directors or a committee of the board identified by the board of directors;
- b) communicate directly and regularly meet (without the presence of senior management) with the chairperson of the board of directors or the committee of the board identified by the board of directors.

6.2.7 The head of a control function shall report in writing to the board of directors, as well as the Commission, any matter relating to the business of the insurer of which the head becomes aware in the performance of his/her functions and which, constitutes a contravention of any section of the Act or a material contravention of any other legislation that applies to the insurer, or any other irregularity that may compromise the interests of policyholders which -

- a) in the case of any material contravention of the Act, be made within 7 days;
- b) in any other case, be made at the first meeting of the board of directors following the contravention; and

- c) where the matter relates to a contravention of the Act, submit the report referred to in a) above, within 60 days to the Commission if, appropriate steps to rectify the matter are not taken by the board of directors to the satisfaction of the head within 30 days after the date in which the report was made to the board of directors.

## 7 Risk Management Function

### 7.1 General Principles

7.1.1 The risk management function shall establish, implement and maintain appropriate mechanisms and activities (including a strategy and operational plan) to –

- a) assist the board of directors and management in carrying out their respective responsibilities, including by providing specialist analysis and performing risk reviews;
- b) identify, measure, monitor and manage the risks the insurer faces;
- c) gain and maintain an aggregated view of the risk profile of the insurer at an enterprise wide and individual business unit level;
- d) evaluate the internal and external risk environment on an on-going basis in order to identify and assess potential risks as early as possible;
- e) consider risks arising from remuneration arrangements and incentive structures within the insurer and in respect of persons to whom activities have been outsourced;
- f) conduct regular stress testing and scenario analyses, including in respect of outliers or matters with low probability but high potential impact;
- g) regularly report to management, heads of control functions and the board on the insurer's risk profile, and the details of the risk exposures facing the insurer and related mitigation actions;
- h) report material changes affecting the insurer's risk management system to the board of directors to help ensure that the framework is maintained and improved; and
- i) conduct regular assessments of the risk management function and the risk management system and implement or monitor the implementation of any needed improvements.

7.1.2 The risk management system shall be reviewed regularly by the internal audit function or an independent and objective external party of the insurer to ensure that the system remains

effective and that any necessary modifications are identified and effected in a timely manner.

7.1.3 The risk management function shall promptly inform the board of directors of any circumstance that may have an adverse material effect on the risk management system of the insurer.

7.1.4 The risk management function shall have access to and report to the board of directors or a committee of the board identified by the board of directors on - a) the strategy of the risk management function;

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

c) information on the risk management function's resources, including an analysis on the appropriateness of these resources;

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

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

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

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

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

7.1.5 For insurers who are part of a group, they shall be required to-

a) conduct risk management on a group-wide basis as well as on a legal entity basis;

b) ensure appropriate governance exists across the group; and

c) ensure material information is delivered to all relevant management and the board in a timely manner on a group-wide and legal entity basis.

## 7.2 Risk Responsibilities of Management and the Board of Directors

7.2.1 Management shall have responsibility for implementing the risk management system that has been approved by the board. In implementing the system, management shall have responsibility for translating the risk appetite expressed by the board into a system of risk limitation strategies and controls.

7.2.2 The board of directors is ultimately responsible for the insurer's risk management system and for ensuring that the insurer has in place effective systems and functions to address the material risks it faces.

7.2.3 The board of directors shall have responsibility for-

- a) Defining the insurer's risk appetite in line with the insurer's financial resources, business strategies, management expertise and overall willingness to take risk.
- b) Reviewing and approving the risk management policies and procedures.
- c) Reviewing the risk management system, considering changes in the risk profile of the business (changes in products, markets, operating environment).
- d) Ensuring that the risk management framework is regularly reviewed by appropriately trained and competent personnel that are operationally independent of the risk management activities.

### 7.3 Risk Management Reporting Requirements

7.3.1 The head of the risk management function shall have the authority and obligation to inform the board promptly of any circumstance that may have a material effect on the risk management system of the insurer and detrimental impact to the insurer or its policyholders. The chairman of the board will be required to report to IPEC of any such occurrence.

7.3.2 The board shall provide IPEC with a risk management declaration within ninety (90) days after the end of the insurer's financial year indicating that-

- a) The insurer has systems in place for the purpose of ensuring compliance with this directive;
- b) The board is satisfied with the efficacy of the processes and systems surrounding the production of financial information of the insurer;
- c) The insurer has in place a risk management strategy, developed in accordance with the requirements of this directive, setting out its approach to risk management; and
- d) The systems that are in place for managing and monitoring risks, and the risk management system, are appropriate to the insurer, having regard to such factors as the size, business mix and complexity of the insurer's operations.

## 8 Compliance Function

### 8.1 General Principles

- 8.1.1 Insurers shall be required to have an effective compliance management system capable of assisting the insurer to meet its internal and external obligations. The compliance management system shall promote and sustain a corporate culture of compliance and integrity.
- 8.1.2 The board shall ensure that the insurer complies with all applicable laws, regulations, supervisory decisions and internal policies, and conducts its business ethically and responsibly.
- 8.1.3 The insurer shall have in place a robust well positioned, resourced and properly authorised and staffed compliance function.
- 8.1.4 The compliance function shall provide the board with independent assurance in respect of the insurer's governance, including its risk management and internal controls. The "Three lines of defence" model outlined in this directive provides a benchmark model for good corporate governance.
- 8.1.5 The compliance function shall be required to be independent from management and not be involved operationally in the business.
- 8.1.6 An effective compliance function shall be headed by a suitably experienced and qualified person, having regard to such factors as the size, business mix and complexity of the insurer's operations.
- 8.1.7 The compliance management system shall be reviewed, at most, every three (3) years by the internal audit function or an independent and qualified objective external reviewer of the insurer to ensure that the system remains effective and that any necessary modifications are identified and effected in a timely manner. The reports compiled after the reviews shall be filed with the Commission within a specified period.

### 8.2 General Compliance Responsibilities

- 8.2.1 In order to effectively identify and actively prevent and eliminate compliance risk and ensure sound and stable business operation, an insurer shall establish an effective compliance management system, improve the organizational structure of compliance management and clarify compliance management responsibilities within the organisation.

8.2.2 All staff in an insurer shall be responsible for compliance. An insurer shall boost and cultivate a good compliance culture, enhance the compliance awareness of all employees including marketing staff, and regard the compliance culture construction as an important part of the construction of the corporate culture.

8.2.3 Management shall set the tone for compliance from the top. The board of directors and the management-

- a) shall advocate ethics and values of honesty and good faith;
- b) shall advocate such philosophies as voluntary compliance and compliance bringing about values; and
- c) shall make internal compliance management and external supervision better interact with each other.

### 8.3 Compliance Function Responsibilities

8.3.1 The compliance function shall establish, implement and maintain appropriate mechanisms and activities to -

- a) assist the board of directors and senior management in carrying out their respective responsibilities;
- b) establish, implement and maintain a risk-based compliance plan;
- c) promote a compliance culture that values responsible conduct and compliance with internal and external obligations;
- d) identify, assess and report on key legal and regulatory obligations and the risks associated therewith, including obligations under the Act and any other applicable laws;
- e) assess the appropriateness of policies, processes, and controls in respect of key areas of internal and external obligations including, legal, regulatory, and ethical obligations and the effective monitoring thereof by the insurer;
- f) ensure that regular training is conducted on key internal, legal and regulatory obligations particularly for employees in positions of trust or responsibility or who are involved in activities that have significant legal or regulatory risk;
- g) facilitate the confidential reporting by employees of concerns, shortcomings or potential non-compliance in respect of the insurer's policies, legal or regulatory obligations, or ethical considerations;

- h) monitor instances of non-compliance, and ensuring that adequate disciplinary actions are taken where appropriate and any necessary reporting to the Commission or other relevant regulatory authorities is made; and
- i) conduct regular assessments of the compliance function and the compliance policies and systems and implement or monitor needed improvements.

#### 8.4 Compliance Responsibilities of the Board

8.4.1 The board of directors is ultimately responsible for the effectiveness of the insurer's compliance management and shall perform the following compliance duties-

- a) Deliberating and verifying the annual and semi-annual compliance report of the insurer;
- b) Examining and approving compliance policies, supervising their implementation and evaluating their implementation annually;
- c) Examining and approving the annual compliance report of the company, presenting such report to IPEC and taking measures to settle non-compliance referred to in such a report;
- d) Approving such issues as the appointment, dismissal and remuneration of the head of compliance function;
- e) Approving the structure and responsibilities of the compliance function;
- f) Ensuring that the head of the compliance function can independently communicate with the board of directors, the audit committee or any other special committee of the board; and
- g) Other compliance duties as stipulated in the articles of association of the insurer.

8.4.2 The board shall grant suitable authority to the compliance function, including authority to-

- a) Access and review any records or information of the insurer which the compliance function deems necessary to carry out its reviews;
- b) Undertake on the compliance function's initiative, a review of any area or any function consistent with its mission;
- c) Require appropriate management responses to compliance reports, including development of a suitable remedial action; and

- d) Decline doing a review, or taking on any other responsibilities requested by management, if the compliance function believes this is inconsistent with its mission or with the strategy and compliance plan approved by the board. In any such case, the compliance function shall inform the board and seek its guidance.

8.4.3 The insurer may, in light of its actual situation, appoint other special committees set up by the board of directors to perform the compliance duties specified above.

## 8.5 Compliance Responsibilities of the Principal Officer

8.5.1 The principal officer of an insurer shall perform the following compliance duties in accordance with the decisions made by the board of directors-

- a) setting up and improving the compliance management organization structure;
- b) appointing, subject to the approval of the board, the head of the compliance function to the board of directors;
- c) establishing the compliance function;
- d) providing sufficient conditions for the compliance function to perform its duties;
- e) Examining the compliance policies presented by the head of the compliance function and exercising them upon approval of the board of directors;
- f) Through the head of compliance function, identifying and evaluating compliance risks of the insurer at least semi-annually as well as verifying the compliance risk management plan of the next year;
- g) Verifying the annual and semi-annual compliance reports and submitting them to the audit committee of the board of directors;
- h) After finding out any non-compliant operational and management behaviour, promptly taking remedial measures; and
- i) Other compliance duties that are stipulated in the articles of association or determined by the board of directors.

8.5.2 The heads of units, general manager of a branch office or central sub-branch of the insurance company shall promptly take remedial measures after noting any noncompliance issues.

## 8.6 Compliance Reporting Requirements

8.6.1 An insurance company shall set down compliance policies and shall submit them to IPEC after they are deliberated on and approved by the board of directors.

8.6.2 A compliance policy, shall at least contain the following -

- a) The company's objective and basic principles of compliance management;
- b) The compliance culture advocated by the company;
- c) The compliance duties assumed by the board of directors and senior managers;
- d) The framework of compliance management and routes for reporting information;
- e) The status and duties of the compliance department; and
- f) The major procedures for identifying and managing compliance risk.

8.6.3 An insurance company shall, on an annual basis, evaluate its compliance policies and shall, in light of the actual needs, revise them.

8.6.4 The head of the compliance function shall have access to and report to the board and/or relevant committees or sub-committees on matters such as;

- a) Formulation, evaluation and revision of compliance policies;
- b) An assessment of the key compliance risks the insurer faces and the steps being taken to address them;
- c) An assessment of how the various parts of the insurer (e.g. divisions, major business units, product areas) are performing against compliance standards and goals;
- d) 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;
- e) Fines or other disciplinary actions taken by the Commission or any regulator in respect of the insurer or any employee;
- f) Any factors that may be adversely affecting the compliance function's independence, objectivity or effectiveness;
- g) Compliance trainings; and
- h) Other issues as deemed necessary

8.6.5 The head of the compliance function shall have the authority and obligation to promptly inform the chairperson of the board directly in the event of any contravention of the Insurance Act [Chapter 24:07] and any other major non-compliance by a member of management or any staff member for that matter or a material non-compliance by the insurer with an external obligation. This shall apply where he or she believes that

management is not taking the necessary corrective actions and a delay would be detrimental to the insurer or its policyholders.

8.6.6 The chairman of the board will be required to report to IPEC any such occurrence and institute an investigation and/or remedial action within seven (7) days

8.6.7 The board shall provide IPEC with a compliance function declaration within three (3) months after the closure of the insurer's financial year stating that, to the best of its knowledge and belief, having made appropriate enquiries-

- a) The insurer has systems in place for the purpose of ensuring compliance with this directive; and
- b) The systems that are in place for managing and monitoring risks, and the compliance function, are appropriate to the insurer, having regard to such factors as the size, business mix and complexity of the insurer's operations.

## 9 Actuarial function

### 9.1 Role of the Actuarial Function

9.1.1 The actuarial function shall provide assurance to the board of directors regarding the accuracy of the calculations and the appropriateness of the assumptions underlying the insurance liabilities and the capital adequacy requirement by, at least, performing the following functions-

- a) Assessing and valuation of the insurer's insurance liabilities, including policy provisions and aggregate claim liabilities, as well as determination of reserves for financial risks;
- b) Assisting the insurer with asset liability management with regards to the adequacy and the sufficiency of assets and future revenues to cover the insurer's obligations to policyholders and capital requirements, as well as other obligations or activities;
- c) Evaluating the insurer's investment policies and the valuation of assets;
- d) Establishing an insurer's solvency position, including a calculation of minimum capital required for regulatory purposes and liability and loss provisions;
- e) Conducting Own Risk and Solvency Assessment (ORSA) i.e. capital adequacy assessments and stress tests under various scenarios, and measuring their relative

impact on assets, liabilities, and actual and future capital. ORSA shall also be conducted after significant developments such as mergers and acquisitions, launch of new products etc.;

- f) the fair treatment of policyholders with regard to distribution of profits awarded to participating policyholders;
- g) the adequacy and soundness of underwriting policies;
- h) the development, pricing and assessment of the adequacy of reinsurance arrangements;
- i) pricing of insurance products, along with estimation of the capital required to underwrite the product;
- j) the sufficiency, accuracy and quality of data, the methods and the assumptions used in the calculation of technical provisions;
- k) the research, development, validation and use of internal models for internal actuarial or financial projections, or for solvency purposes as in the ORSA; and
- l) any other actuarial or financial matters determined by the reviewing and attesting to the reliability and adequacy of the insurance liabilities and the capital adequacy requirement, including by –
  - i. ensuring the appropriateness of the methodologies and underlying models used and assumptions made;
  - ii. assessing the sufficiency and quality of the data used in the calculations;
  - iii. comparing best estimates, as well as prudent estimates against experience when evaluating liabilities;
  - iv. informing the board of directors of the reliability and adequacy of the calculations;
  - v. overseeing the calculations in the cases where, due to insufficient data of appropriate quality to apply reliable actuarial method, approximations were used in the calculation of liabilities and the capital adequacy requirement;
  - vi. expressing an opinion on the asset-liability management policy and the underwriting risk management policy;
  - vii. expressing an opinion on the reinsurance and other forms of risk transfer policy and the adequacy of reinsurance arrangements; and

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

9.1.2 Subsection (9.1.1.) does not apply where the Appointed Actuary in terms of section 9.2 of these directives performs the responsibilities and functions of the actuarial function.

## 9.2 Appointed Actuary

9.2.1 The board of the insurer has the responsibility of appointing a suitably qualified actuary for the role of Appointed Actuary upon obtaining approval from IPEC who will apply a “fit and proper” test to such appointment.

9.2.2 The Appointed Actuary shall have the qualification of Fellow of The Institute and Faculty of Actuaries UK, or equivalent and shall be a member of the Actuarial Society of Zimbabwe.

9.2.3 The Appointed Actuary shall not hold positions within or outside of the insurer that may create conflicts of interest or compromise his or her independence. The board of the insurer shall determine whether the Appointed Actuary has any potential conflicts of interest, such as if his or her firm also provides audit services to the insurer. If any such conflicts exist, the board shall subject them to appropriate controls subject to approval by IPEC or order other arrangements.

9.2.4(a) If an Appointed Actuary resigns or is replaced, the insurer shall notify IPEC and give the reasons for the resignation or replacement. Such a notification shall include a statement from the insurer of whether there were any disagreements with the former Appointed Actuary over 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.

b) An external Actuary shall be appointed or shall save a maximum of five (5) years. Reappointment of the same Actuary is subject to a cooling off period of three (3) years.

9.2.5 The Appointed Actuary shall submit to the board-

a) an Actuarial Function Report (AFR) within two months of the end of each financial year; and

b) a half yearly solvency statement determined in accordance with the insurer’s as well as regulatory solvency guidelines and generally accepted actuarial principles.

9.2.6 The insurer shall submit to IPEC -

a) an AFR within three (3) months of the end of each financial year; and

b) a quarterly solvency statement determined in accordance with the insurer's as well as regulatory solvency guidelines and generally accepted actuarial principles at the end of each quarter to IPEC.

9.2.7 The Appointed Actuary shall report to IPEC directly and within one (1) month in circumstances-

a) where the insurer has breached, or is likely to breach solvency requirements for both the regulator and the insurer;

b) where the insurer has ceased holding effective reinsurance cover;

c) where an insurer or its directors may have contravened the Act or any other law and the contravention may prejudice the interests of the policyholders; and

d) Any other circumstances have been established that will compromise the insurer's ability to meet policyholder obligations

9.2.8 Where such a report is made directly to IPEC, the Appointed Actuary is not under any obligation to disclose this to the management and/or the board of the insurer if the Appointed Actuary considers that by doing so, the interests of policyholders may be jeopardised or has lost confidence in the board or Management of the company.

9.2.9 IPEC may require an entity to replace an Appointed Actuary if such a person fails to perform required duties or is deemed not "fit and proper." IPEC may also bar such an Actuary from operating in Zimbabwe

### 9.3 Actuarial Function Report

9.3.1 The Appointed Actuary shall produce a written report to be submitted to the board at least annually. The report shall document the tasks that have been undertaken by the Actuarial Function (AF) and their results and shall clearly identify any deficiencies and give recommendations as to how such deficiencies shall be remedied. More specifically-

9.3.2 The AFR shall contain an Executive Summary which summarises the most important elements of the report and its conclusions.

9.3.3 The AFR shall express a conclusion from the AF on the adequacy and reliability of technical provisions

9.3.4 Where the AFR concludes that the technical provisions are either inadequate or unreliable, a summary of the key concerns and recommendations shall be included in the conclusion.

9.3.5 The AFR shall express a conclusion on the underwriting policy and whether it reflects and is

consistent with the risk appetite of the company. Where any shortcomings are identified, a summary of the key concern and recommendations shall be included in the conclusion.

9.3.6 The AFR shall have an assessment of reinsurance policy and whether it is consistent with the risk appetite of the insurer. Where any shortcomings are identified, a summary of the key areas of concerns and recommendations shall be included in the conclusion.

9.3.7 In formulating, professional conclusions, the AF shall be objective and free from influence of other functions or of the board and shall provide its opinion in an independent fashion.

9.3.8 The AFR shall document a summary of all major tasks that have been undertaken by the AF and their results.

9.3.9 The AFR shall clearly identify any deficiencies and give recommendations as to how such deficiencies shall be remedied.

9.3.10 The level of detail of the AFR shall be dependent on nature, scale and complexity of the underlying risks of the undertaking. (Principle of Proportionality)

9.3.11 The AFR shall include sufficient information and discussion about each area covered so as to enable the board to judge its implications.

9.3.12 The AFR shall provide information to demonstrate that each of the writers of the AFR, and, if applicable, the person taking overall responsibility for the AFR, has the relevant knowledge and experience to fulfil the role.

9.3.14 The AFR shall include a description of the main responsibilities and tasks of the actuarial function, including any which are not required by this directive.

9.3.15 The AF shall consider the preference of the insurer's board on depth of reporting and on the potential inclusion of additional topics in the AFR. This standard does not prevent areas not specifically referred to in this directive appearing in the AFR.

9.3.16 The AFR shall set out information identifying relevant conflicts of interest and describing how they have been managed.

9.3.17 The AF shall disclose any material reliance on other work and how the AF gained assurance on the reliability of the other work.

9.3.18 Details of whether recommendations in the AFR have been accepted, and, if so, on progress towards implementation, shall be summarised in the next AFR.

9.3.19 The AFR may explicitly state that it is in compliance with this standard.

9.3.20 The following areas shall also be given appropriate attention within the AFR;

a) Data used

- i) Key data used in carrying out the exercise shall be disclosed as well as the sources of this information. The AFR shall comment on the level of accuracy and reliance placed on data used in carrying out the exercise. Any material limitations and adjustments made to the data shall also be disclosed.
- ii) The AFR shall draw attention to any material areas of uncertainty and their sources, and also any material judgements made in the assessments by the AF.

b) Estimation of Technical Provisions

- i) The Actuarial Function shall assess the appropriateness of different methods and procedures in estimating the technical provisions considering the entity, data availability, and different lines of business being underwritten. All methods used shall be disclosed sufficiently and justified appropriately in the AFR.
  - ii) Where different business classes are underwritten; their classification and groupings for technical provisions estimation purposes shall be disclosed. This shall be in line with regulatory guidelines and generally accepted business classifications.
  - iii) Assumptions used shall be disclosed and rationale for their use explained. The Appointed Actuary will develop the assumptions in consultation with the board. The assumptions shall, inter alia, be appropriate for the business based on key experience investigations and account for knowledge from the insurance market.
  - iv) The Actuarial Function shall assess the movement in provisions over time. They shall identify and explain any material movement from one period to another.
  - v) An assessment shall also be made, where applicable and through back testing exercises, of how the provision estimates compare with emerging experience. The actuarial function will objectively determine the period for back testing.
  - vi) The uncertainty associated with the technical provisions shall also be commented on. This can be reported in the form of calculated estimation variations or commentary on the level of uncertainty.
  - vii) Sensitivity and Scenario analysis of all key assumptions shall also be made.
  - viii) For financial reporting purposes, the Actuarial Function shall generally estimate the technical provisions in line with IPEC recommended standards from
-

time to time. Any deviations from these shall be justified or disclosed as part of scenario and sensitivity analysis.

c) Assessment of Assets backing Technical Liabilities

- i) The Actuarial Function shall comment on the appropriateness of the entity's investments and investment policies in light of the nature, term and currency of its Liabilities.
- ii) Any material risks arising from mismatch in assets and liabilities shall be commented on. For example, this can be a material increase in level of liquidity risks as a result of mismatching.
- iii) Other entity's assets such as non-investible assets shall also be commented on. These can be in the form of reinsurance and non-reinsurance recoveries.
- iv) Other regulatory investment guidelines shall also be taken into consideration and comments relating to compliance with prescribed assets made.

d) Opinion on Underwriting Standards and Adequacy of Premiums

- i) The Actuarial Function shall provide an overall opinion on the underwriting policy. This includes adequacy of the new business premium rates, underwriting and claims management standards being used by the entity. In case of short-term contracts, there shall be commentary of the sufficiency of unearned premiums to cover for future claims and expenses taking into account underlying risks and any options and guarantees that may be available.
- ii) The opinion shall cover an assessment of the variability surrounding expected profitability and consistency of variability with risk appetite. The report shall cover an assessment of the entity's response to changing experience. It shall also comment on anti-selection risk.
- iii) The report shall assess consistency of the underwriting policy with other policies as well as consistency of underwriting assumptions with those used for technical provisions and reinsurance.
- iv) An overall comment on relationship between business plan and risk appetite will also be covered.

- v) The Actuarial Function opinion shall strive to provide an opinion that is independent of the influence of other functions including administrative, management and supervisory bodies.
- e) Appropriateness of Reinsurance
- i) The Actuarial Function shall provide an independent assessment of the appropriateness of the current reinsurance or retrocession or any alternative risk transfer arrangements in light of the entity's liability profile.
  - ii) The report shall provide recommendations to improve on reinsurance arrangements, including advantages and disadvantages of any alternatives. The opinion shall assess consistency with risk appetite, risk profile, underwriting policy and technical provisions. It shall include an assessment response under stress tests, e.g. for catastrophe claims, risk aggregations.
  - iii) The level of credit risk associated with these shall also be commented on. This can be in the form of credit ratings or level of diversification in intra-group reinsurance arrangements or other entities or institutions within a corporate group setting.
- f) Solvency Position and Capital Management Assessments
- i) The Actuarial Function shall comment on the level of solvency of the entity considering the stipulated minimum capital requirements and any directives on capital management.
  - ii) Assessment shall also be made on the ability of the insurer to remain solvent based on trend analysis and any forecasts that can be carried out. These assessments will need to be appropriate for the insurance setup. Any material risks that may affect the solvency position of the entity shall also be disclosed.
- g) Key experience investigations
- The AFR shall also contain an analysis of key experiences for the entity. Impact of any changes in assumptions from the previous report, new data/information that was not part of previous investigation shall be highlighted.
- h) Risk management
- i) The Actuarial Function shall comment on any material risks arising from the risk management framework of the insurer.

- ii) The report shall include description of areas of material contribution to risk management, including contribution to risk modelling underlying calculation of capital requirements. Recommendations shall be clearly laid out.
  - iii) An opinion shall be expressed to the board on range of risks and adequacy of scenarios, including financial projections.
  - iv) Any limitations in the ability of the function to comment on such risks for example, due to lack of access or exposure to the risk management strategies or practice of the entity shall also be commented on.
- i) Other AFR details
- i) The name, qualifications and primary regulator of the Appointed Actuary, date report produced, period over which the report relates and details of any other third parties who aided in the production of the report shall be disclosed. Any actuarial guidelines from professional bodies used shall also be indicated.
  - ii) Major conclusions for the major findings shall also be discussed. Key recommendations for addressing and improving on solvency as well as risk management strategies of the entity shall also be discussed. A review of the previous report's recommendations and extent to which they were implemented shall also be discussed.

## 10 Internal Audit Function

### 10.1 General Principles

#### 10.1.1 The Internal audit function shall at least, -

- a) establish, implement and maintain a risk-based audit plan;
- b) review and evaluate the adequacy and effectiveness of the insurer's policies and processes and the documentation and controls in respect of these;
- c) review levels of compliance with established policies, processes, and controls;
- d) evaluate the reliability and integrity of information;
- e) monitor that the identified risks and the agreed actions to address them are accurate, complete and current;

- f) evaluate the internal controls relating to governance, operations and information systems in place to verify the safeguarding of insurer and policyholder assets;
- g) evaluate the effectiveness of the governance framework; and
- h) evaluate the adequacy and effectiveness of the insurer's risk management, compliance and actuarial functions.

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

- a) market, insurance, credit, liquidity, operational (including insurance fraud), and regulatory and compliance (including reputational) risk;
- b) accounting and financial policies and whether the associated records are complete and accurate;
- c) In collaboration with the compliance function, the extent of compliance by the insurer with applicable laws, regulations, rules, and directives from all relevant regulatory authorities;
- d) intra-group transactions, including intra-group risk transfer and internal pricing;
- e) adherence by the insurer to the insurer's remuneration policy;
- f) the reliability and timeliness of escalation and reporting processes, including whether there are confidential means for employees to report concerns or noncompliance, and whether these are properly communicated, offer the reporting employee adequate protection from retaliation, and result in appropriate follow up; and
- g) the extent that any non-compliance with internal policies or external legal or regulatory obligations are documented, and appropriate corrective or disciplinary measures are taken, including in respect of individual employees involved.

10.1.3 The internal audit function shall have access to and, at least annually, report to the board of directors or the audit committee on – a) the strategy of the function;

- b) the function's audit plan, detailing the proposed areas of audit focus;
- c) an assessment on the extent of achievement of the goals set out in the audit plan;
- d) information on its resources, including an analysis on the appropriateness of those resources;

- e) any factors that may impinge on the internal audit function's independence, objectivity, or effectiveness;
- f) material findings from audits or reviews conducted;
- g) material deficiencies of the internal control system, or of compliance with internal policies and procedures or external legal or regulatory obligations, and include agreed management action to remedy all identified deficiencies.; and
- h) the extent of management compliance and progress with previously agreed upon corrective or risk mitigating measures.

## 10.2 Reporting Requirements

10.2.1 The head of the internal audit function shall report functionally to the board or to the audit committee and administratively to the principal officer.

10.2.2 In its reporting, the internal audit function shall cover matters such as-

- a) The function's annual or other periodic audit plan, detailing the proposed areas of audit focus;
- b) Any factors that may be adversely affecting the internal audit function's independence, objectivity or effectiveness;
- c) Material findings from audits or reviews conducted; and
- d) The extent of management's compliance with agreed upon corrective or risk mitigating measures in response to identified control deficiencies, weaknesses or failures, compliance violations or other lapses.

10.2.3 In addition to periodic reporting, the head of internal audit shall be authorised to communicate directly, and meet periodically, with the head of the audit committee or the chairperson of the board without the presence of management.

10.2.4 The internal audit function in addition submitting the report to the board of the insurer, shall also furnish IPEC with an audit report detailing its findings within thirty days after conduct of an audit of any function. However, shall there be material issues which prejudice policyholders or threaten viability of the insurer the internal audit shall immediately report to the Commission.

10.2.5 The board shall provide IPEC with an internal audit declaration within ninety (90) days after the closure of the insurer's financial year stating that, to the best of its knowledge and belief, having made appropriate enquiries that-

- a) The insurer has systems in place for the purpose of ensuring compliance with this directive;
- b) The systems that are in place for managing and monitoring risks, and the internal audit function, are appropriate to the insurer, having regard to such factors as the size, business mix and complexity of the insurer's operations.

10.2.6 The Head of Internal Audit Function shall be expected to be a member of the local Chapter of the Institute of Internal Auditors Zimbabwe or strive to join the same within a period of one two years from the effective date of this framework.

## 11 Outsourcing

### 11.1 General Principles

11.1.1 For the purposes of application of this section, the term outsourcing shall apply to any services provided by any external legal person, including companies related to the insurer in question such as group company. An insurer shall assess the degree of materiality in outsourcing to different service providers. The extent and degree to which this directive is implemented is expected to be commensurate with the materiality of the outsourcing. In assessing materiality, IPEC recognises that qualitative judgement is involved and the circumstances faced by individual insurers may vary. Factors that an insurer shall consider include, among others-

- a) Importance of the business activity to be outsourced, for example, in terms of contribution to income and profit;
- b) Potential impact of the outsourcing on earnings, solvency, liquidity, funding and capital, and risk profile;
- c) Impact on the insurer's reputation and brand value, and ability to achieve its business objectives, strategy and plans, shall the service provider fail to perform the service;
- d) Aggregate exposure to a particular service provider in cases where the insurer outsources various functions to the same service provider; and
- e) Ability to maintain appropriate internal controls and meet regulatory requirements, if there were operational problems faced by the service provider.

11.1.2 While insurers will consider outsourcing different business management functions to reduce their costs and achieve strategic objectives, care will need to be taken on the activities outsourced to different service providers.

11.1.3 As in line with the “Three Lines of Defence” model, there is need to maintain some degree of independence to ensure different functions which are meant to be independent are not carried out by the same service provider. For example, if the internal audit function and the actuarial function are outsourced to the same service provider it may compromise the role of these functions.

11.1.4 Where such is to be allowed, there shall be clear policies to safeguard and ensure the desired degree of independence is maintained.

11.1.5 An insurer shall undertake periodic reviews of its outsourcing arrangements to identify new material outsourcing risks as they arise.

11.1.6 An agreement which was previously not material may subsequently become material from incremental activities outsourced to the same service provider or an increase in volume or nature of the activity outsourced to the service provider.

11.1.7 Material outsourcing risks may also arise when the service provider in a material outsourcing plans to sub-contract the service or makes significant changes to its subcontracting arrangements.

11.1.8 An insurer shall consider materiality at both the insurer and on a consolidated basis, i.e. together with the insurer’s branches and corporations under its control.

## 11.2 Role of the Board and Senior Management

11.2.1 The board and senior management of an insurer retain ultimate responsibility for the effective management of risks arising from outsourcing.

11.2.2 The Principal Officer shall be responsible for seeking approval of the outsourcing arrangements from the Commission once the insurer has made the decision to outsource. The Commission shall apply fit and proper assessment criteria in making its decision.

11.2.3 While an insurer may delegate its day-to-day operational duties to the service provider, the responsibilities for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions, continue to rest with the insurer, its board and senior management. The insurer, or a committee delegated by it, is responsible for-

- a) approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing and the policies that apply to such arrangements;

- b) laying down the appropriate approval authorities for outsourcing depending on the nature of risks in, and materiality of the outsourcing;
- c) assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures as commensurate with the nature, scope;
- d) complexity of the outsourcing arrangements;
- e) undertaking regular review of outsourcing strategies and arrangements for their continued relevance, and safety and soundness; and
- f) reviewing a list of all material outsourcing and relevant reports on outsourcing.

#### 11.2.4 Senior management is responsible for-

- a) Evaluating the risks and materiality of all existing and prospective outsourcing, based on the framework approved by the board;
- b) Developing and implementing sound and prudent outsourcing policies and procedures commensurate with the nature, scope and complexity of the outsourcing;
- c) Reviewing periodically the effectiveness of policies and procedures;
- d) Communicating information pertaining to material outsourcing risks to the board in a timely manner;
- e) Ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and tested; and
- f) Ensuring that there is independent review and audit for compliance with set policies.

### 11.3 Capability of Service Providers

11.3.1 In considering, renegotiating or renewing an outsourcing arrangement, an insurer shall subject the service provider to appropriate due diligence to assess its capability to employ a high standard of care in performing the service and comply with its obligations under the outsourcing agreement.

11.3.2 The due diligence shall take into consideration qualitative and quantitative, financial, operational and reputation factors. Compatibility and performance shall be emphasized in the assessment. Where possible, the insurer shall obtain independent reviews and market feedback on the service provider to supplement its own findings.

11.3.3 The due diligence shall involve an evaluation of all available information about the service provider such as-

- a) Establishing, implementing and maintaining a risk-based audit plan to examine and evaluate general or specific areas, including on a preventive basis;
- b) its experience and competence to implement and support the proposed activity over the contracted period;
- c) its financial strength and resources where applicable (the due diligence shall be similar to a credit assessment of the viability of the service provider based on reviews of business strategy and goals, audited financial statements, the strength of commitment of significant equity sponsors and ability to service commitments even under adverse conditions);
- d) its business reputation and culture, compliance, complaints and outstanding or potential litigation;
- e) its security and internal controls, audit coverage, reporting and monitoring environment;
- f) its business continuity management;
- g) its reliance on and success in dealing with sub-contractors;
- h) its insurance coverage; and
- i) its external factors (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates, and other events) that may impact service performance.

11.3.4 Due diligence undertaken during the selection process shall be documented and reperformed periodically (At least annually) as part of the monitoring and control processes of outsourcing.

11.3.5 The due diligence process can vary depending on the nature of the outsourcing arrangement e.g. reduced due diligence may be sufficient where no developments or changes have arisen to affect an existing outsourcing arrangement or where the outsourcing is to a member of the group.

11.3.6 An insurer shall ensure that the information used for due diligence evaluation is current and shall not be more than 12 months old.

#### 11.4 Outsourcing Agreement

11.4.1 Contractual terms and conditions governing relationships, functions, obligations and responsibilities of the contracting parties in the outsourcing shall be carefully and properly defined in written agreements.

11.4.2 The detail in these agreements shall be appropriate for the nature and materiality of the arrangement. They shall also be vetted by a competent authority e.g. the insurer's legal counsel on their legal effect and enforceability.

11.4.3 An insurer shall ensure that every outsourcing agreement addresses the risks and risk mitigation strategies identified at the risk evaluation and due diligence stages. Each agreement shall allow for renegotiation and renewal to enable the insurer to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet its legal and regulatory obligations.

11.4.4 The agreement shall also not hinder IPEC in the exercise of its supervisory powers over the insurer and right of access to information on the insurer and the service provider. It shall at the very least, have provisions pertaining to-

a) The scope of the outsourcing service; and

b) Performance standards defined in terms of, for example, service levels and performance targets; service availability, reliability, stability and upgrade;

#### 11.5 Confidentiality and Security

11.5.1 As public confidence in insurers is a cornerstone in the stability and reputation of the insurance industry, it is vital that an insurer satisfies itself that the service provider's security policies, procedures and controls will enable the insurer to protect confidentiality and security of customer information;

#### 11.6 Business Continuity Management

11.6.1 An insurer shall ensure that its business continuity preparedness is not compromised by outsourcing. In that regard, an insurer shall take steps to evaluate and manage the interdependency risk arising from the outsourcing arrangement such that the insurer remains able to conduct its business smoothly in the event of disruption, unexpected termination of the outsourcing or liquidation of the service provider.

11.6.2 These shall include steps to;

a) Determine that the service provider has in place satisfactory business continuity plans (BCP) commensurate with the nature, scope and complexity of the outsourcing.

- b) Proactively seek assurance on the state of BCP preparedness of the service provider.
- c) Ensure the service provider is able to isolate and clearly identify the insurer's information, documents and records, and other assets such that in adverse conditions, all documents, records of transactions and information given to the service provider, and assets of the insurer, can be either removed from the possession of the service provider in order to continue its business operations, or deleted, destroyed or rendered unusable.

#### 11.7 Monitoring and Control

- 11.7.1 An insurer shall establish a structure for the management and control of outsourcing. Such a structure will vary depending on the nature, scope and complexity of the outsourced activity.
- 11.7.2 As outsourcing relationships and interdependencies increase in materiality and complexity, a more rigorous risk management approach shall be adopted. An insurer also has to be more proactive in its relationship with the service provider e.g. having frequent meetings, to ensure that performance levels are upheld.
- 11.7.3 An insurer shall ensure that outsourcing agreements with service providers contain provisions to address their monitoring and control of outsourced activities.

#### 11.8 Audit and Inspection

- 11.8.1 Outsourcing should not interfere with the ability of the insurer to effectively manage its activities or impede IPEC in carrying out its supervisory functions and objectives.
- 11.8.2 Every insurer is therefore required to take steps to ensure that outsourcing agreements with the service provider include clauses that allow-
  - a) The insurer to conduct audits on the service provider, whether by its internal or external auditors, or by agents appointed by the insurer; and to obtain copies of any report and finding made on the service provider in conjunction with the service performed for the insurer; and
  - b) IPEC, or any agent appointed by IPEC, to access both the service provider and the insurer to obtain records and documents, of transactions, and information of the insurer given to, stored at or processed by the service provider and the right to access any report and finding made on the service provider.

#### 11.9 Dispute Resolution

- 11.9.1 Agreements shall specify the resolution process, events of default, and the

- indemnities, remedies and recourse of the respective parties in the agreements;
- 11.10 Default Termination and Early Exit
- 11.10.1 An insurer shall have the right to terminate the agreement in the event of default, including circumstances when the service provider undergoes a change in ownership, becomes insolvent, goes into liquidation, receivership, or judicial management, whether in Zimbabwe or elsewhere; or when there has been a breach of security, confidentiality or demonstrable deterioration in the ability of the service provider to perform the service as contracted.
- 11.10.2 The minimum period to execute a termination provision shall be specified;
- 11.11 Sub-contracting
- 11.11.1 An insurer should retain the ability to maintain similar control over its outsourcing risks when a service provider uses a subcontractor as in its agreement with the service provider.
- 11.11.2 Agreements shall have clauses setting out the rules and limitations on sub-contracting.
- 11.11.3 An insurer may want to include clauses making the service provider contractually liable for the capability of the sub-contractor it selects and for compliance with the provisions in its agreement with the service provider, including the prudent practices set out in this directive, and in particular those relating to security and confidentiality, audit and inspection as well as business continuity management.
- 11.11.4 For material outsourcing arrangements, the sub-contracting of all or substantially all of a service provided, should be subject to prior approval of the insurer.
- 11.12 Applicable Laws
- 11.12.1 Agreements should include choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction.
- 11.12.2 Each agreement should be tailored to address additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when outsourcing to a service provider outside Zimbabwe.

## 11.13 Legal and Regulatory Obligations

11.13.1 Outsourcing does not diminish the obligations of an insurer, and those of its board and

senior management, to comply with relevant laws and regulations in Zimbabwe. Risk management practices should therefore include steps to ensure all relevant laws, regulations, guidelines and other directions, as well as any condition of approval, licensing or registration, continue to be met.

11.13.2 IPEC supervisory powers over insurers and ability to carry out supervisory functions should also not be hindered, whether the service provider is located within Zimbabwe or elsewhere.

11.13.3 Every insurer shall conduct its business with integrity and competence. Hence an insurer shall not engage in outsourcing that results in its internal control, business conduct or reputation being compromised or weakened.

11.13.4 An insurer has to take steps to ensure that the service provider employs a high standard of care in performing the service as if the activity were not outsourced and conducted within the insurer.

11.13.5 The insurer also needs to maintain the capability and appropriate level of monitoring and control over outsourcing, such that in the event of disruption or unexpected termination of the service, it remains able to conduct its business with integrity and competence.

## 12 Enforcement

12.1 Where the Commission considers that violation of the provisions of this directive have been committed, the Commission shall inform the insurer in writing and allow the insurer to make representations in writing on the matter.

12.2 If after considering any representations made by the insurer concerned in terms of 12.1 above, the Commission is satisfied that the insurer has contravened any provisions of this directive the Commission may, do any one or more of the following—

- a) issue a warning to the insurer and issue a written instruction to the insurer to undertake remedial action specified in the instruction;
- b) declare certain persons as not being fit and proper;
- c) require the insurer to appoint a person who, in the Commission's opinion, is qualified to advise the institution on the proper conduct of his or her business;
- d) impose a monetary penalty on the insurer, not exceeding the equivalent of a fine of level four for each day that the contravention has continued;
- e) instruct the insurer to suspend or remove any of his or her directors or employees;
- f) direct the insurer to suspend all or any of its insurance or insurance-related business;
- g) appoint a person to monitor the insurer's affairs;
- h) convene a meeting of the shareholders or other owners of the insurer to discuss the remedial measures to be taken.

12.3 Before taking any action in terms of section 12.2 above, the Commission shall inform the insurer concerned, in writing, of—

- a) the contravention of which he or she is believed to be guilty and, in substance, the grounds for that belief; and
- b) the proposed action in respect of the alleged contravention; and shall afford the insurer an adequate opportunity to make representations in the matter:

Provided that, where the Commission considers that immediate action is necessary to prevent irreparable harm to the insurer or its policy owners, creditors or shareholders, the Commission may take such action before affording the insurer an opportunity to make representations.