SD 0880/10

INSURANCE ACT 2008

CORPORATE GOVERNANCE CODE OF PRACTICE FOR REGULATED INSURANCE ENTITIES

Laid before Tynwald	16 November 2010
Coming into operation	1 October 2010

The Supervisor, after consulting such persons and bodies as appear to him to be appropriate, issues these Guidance Notes under section 51(1) of the Insurance Act 2008 as binding guidance.

Price £5.00

Contents **Page**

1. INTRODUCTION

1.1 Corporate governance

Corporate governance is the system by which the persons who are responsible for the regulated entity direct and control its affairs, and the means by which they are held accountable for their performance and actions. Corporate governance encompasses all aspects relating to the regulated entity's organisation and business including, but not limited to, its constitutional structures and rules, its corporate culture and environment, as well as its business and operational strategies, policies, procedures, internal controls, decision making processes and conduct.

As a framework, corporate governance defines roles, responsibilities and accountabilities. It clarifies who possesses the duty and legal power to act on behalf of the regulated entity and under which circumstances. It sets out rules for decision making and requirements for documenting decisions and actions, along with their rationale, and for making adequate and appropriate disclosures to stakeholders. Furthermore, it provides for corrective action for non-compliance and ineffectual oversight and management. Corporate governance therefore addresses the allocation and oversight of power and accountabilities, as well as the avoidance of undue concentration and inappropriate use of power.

There is no standard model of corporate governance and approaches will differ between entities to take account of their individual circumstances and preferences. However, a regulated entity's corporate governance must recognise and protect the rights of all interested parties, and include active concern with, understanding of and diligent discharge of responsibilities in a sound, prudent and responsible manner. In particular, such governance requires the commitment of the regulated entity's directors and senior managers, both individually and collectively, and their leadership in promoting a supportive internal culture and environment.

1.2 These Guidance Notes in operation

These Guidance Notes are not intended to be, and should not be interpreted as being, exhaustive. They should be viewed as a component part of a regulated entity's means of maintaining and demonstrating adequate and effective corporate governance appropriate to its circumstances. These Guidance Notes do not limit, and therefore should be read in conjunction with, other legal and regulatory requirements applicable to the regulated entity. These Guidance Notes should not be used as a substitute for legal advice.

2. TITLE AND COMMENCEMENT

The title of these Guidance Notes is the Corporate Governance Code of Practice for Regulated Insurance Entities ("the CGC") and they shall come into operation on 1 October 2010.

3. GOVERNANCE REQUIREMENT AND APPLICATION OF THE CGC

3.1 Application of the CGC

Subject to paragraph 3.2, the CGC applies to a person —

(a) authorised under section 8 of the Act;

(b) permitted under section 22 of the Act in relation to that person's activities carried on in or from the Isle of Man; and

(c) registered under section 25 of the Act as an insurance manager.

3.2 Application to permit holders

A person authorised to carry on an insurance business in any Member State of the European Union is exempt from paragraph 3.1(b).

3.3 Governance requirement and implementation of the CGC

A regulated entity shall have in place an appropriate and effective system of governance that provides for its sound and prudent management.

This includes, but is not limited to, its board and senior management establishing, implementing and maintaining appropriate and effective measures that meet the CGC's requirements in a way that is proportionate to the nature, scale and complexity of the regulated entity, its activities and the risks to which it is exposed.

4. DIRECTORS' CERTIFICATE ON CORPORATE GOVERNANCE

A regulated entity shall, at the same time as its annual accounts are submitted to the Supervisor, provide to the Supervisor a completed certificate in the form set out in Schedule 2.

This requirement is applicable to annual accounts for financial periods commencing on or after 1 April 2011.

5. GENERAL GOVERNANCE REQUIREMENTS

5.1 Integrity

A regulated entity shall —

(a) act honestly and in a straightforward manner; and

(b) ensure that it makes clear to those with whom it has dealings in the course of its business, or prospective business, its name and regulatory status appearing on the relevant register kept under section 48 of the Act.

5.2 Compliance

A regulated entity has an obligation to identify and comply with its legal and regulatory obligations and shall take all reasonable steps to do so.

5.3 Care, skill and diligence

A regulated entity shall conduct its business with due care, skill and diligence, and with due regard for the potential consequences of its intended actions.

5.4 Stakeholder interests

A regulated entity, in conducting its business, shall have due regard for the rights, interests and information needs of its stakeholders, and shall take account of those factors within its governance arrangements as necessary to ensure that its stakeholders are treated fairly.

5.5 Financial management

A regulated entity shall manage its capital and other financial resources prudently. Accordingly, it shall —

(a) maintain adequate capital and other financial resources to meet its liabilities that might reasonably be expected to arise out of the risks to which it is exposed;

(b) maintain sufficient asset liquidity to meet the cash flows of those liabilities as they fall due; and

(c) undertake periodic forward-looking analysis of its ability to meet its obligations under various adverse economic and business scenarios to ensure that it adequately covers the risks to which it is exposed.

5.6 General management

A regulated entity shall have an appropriate level of management, with adequate and competent staffing and resources, that provides for its sound and prudent management.

5.7 Asset protection

A regulated entity shall take all reasonable steps to safeguard its assets and any other assets in its keeping.

5.8 Records

A regulated entity shall —

(a) keep proper books, accounts and documents (together "records") appropriate to its business that provide legible, accurate, verifiable, timely, complete and comprehensible information;

(b) maintain those records in a manner that is readily accessible in or from the Isle of Man and available for inspection and investigation by or on behalf of the Supervisor; and

(c) without limiting any other applicable retention requirement, any such record shall be kept for at least six years from the date it is made or, if later, it ceases to be relevant.

5.9 Governance system documentation

A regulated entity shall establish and maintain adequate and appropriate documentation of its significant systems of governance, including its —

(a) governance principles and structures;

(b) strategies, policies, procedures and internal controls; and

(c) decision making processes.

5.10 Business continuity

A regulated entity shall take all reasonable steps to reduce the likelihood, impact and possible duration of disruption to the continuity of its operations and establish, implement and maintain adequate and appropriate arrangements to ensure that it can continue to function effectively and comply with its legal and regulatory obligations (as identified in accordance with paragraph 5.2) in the event of anticipated or unforeseen disruption.

6. BOARD COMPOSITION AND OPERATION

6.1 Appointment and removal of directors

A regulated entity shall establish, implement and maintain a documented and transparent board nomination, election and removal process.

6.2 Board composition

(a) The board of a regulated entity shall include an adequate number of directors with an appropriate overall combined level of knowledge, skills, experience and commitment such that it can properly discharge its duties and responsibilities and carry out its functions in relation to the regulated entity.

(b) Subject to paragraphs (c) to (e), the board of a regulated entity shall include at least —

(i) one independent non-executive director; and

(ii) two directors who are resident in the Isle of Man.

(c) The requirement under paragraph (b)(ii) is reduced such that the board of a regulated entity that —

(i) is dormant; or

(ii) has appointed an insurance manager registered under section 25 of the Act to manage its day to day operations,

shall include at least one director who is resident in the Isle of Man.

(d) A regulated entity that —

(i) is dormant;

(ii) is a person registered under section 25 of the Act; or

(iii) has obtained the Supervisor's written approval to be so exempt,

is exempt from paragraph b(i).

(e) A regulated entity permitted under section 22 of the Act is exempt from paragraph b(ii).

Where the relevant requirements are met in each case, a director referred to in paragraph (b)(i) may be the same individual as a director referred to in paragraph (b)(ii) or (c).

6.3 Objective oversight and judgement

The board of a regulated entity shall be able to exercise an appropriate degree of objective oversight and judgement in the affairs of the regulated entity.

6.4 Chairman and chief executive

Where a regulated entity has appointed a chairman and a chief executive (or equivalent) then, ordinarily, those posts shall not be combined in one individual within the same regulated entity.

However, if for any reason the posts of chairman and chief executive (or equivalent) are combined, the board of the regulated entity shall —

(a) establish and maintain adequate and appropriate internal controls to ensure that the management of the regulated entity is held effectively accountable to the board; and

(b) at appropriate intervals, and at least annually, review —

(i) the reasons for combining the posts of chairman and chief executive to ensure they remain valid; and

(ii) the internal controls established under paragraph (a) to ensure they remain adequate, appropriate and effective.

6.5 Powers of the board

The board of a regulated entity shall have adequate and appropriate powers and resources so it can properly discharge its duties and responsibilities and carry out its functions in relation to the regulated entity. For this purpose the board shall, amongst other things, be able to —

(a) obtain timely, accurate, relevant and sufficiently comprehensive information and analyses relating to the regulated entity, its management and external environment;

(b) delegate its functions as appropriate; and

(c) obtain external expertise where necessary and as appropriate.

6.6 Matters reserved to the board

The board of a regulated entity shall —

(a) establish and maintain a formal, written schedule which clearly sets out those matters that are specifically reserved for the board's decision in relation to the regulated entity; and

(b) monitor and review at appropriate intervals, and at least annually, the range and focus of the matters specified in that schedule to ensure they remain adequate and appropriate so the board can properly discharge its duties and responsibilities and carry out its functions in relation to the regulated entity.

6.7 Frequency of board meetings

The board of a regulated entity shall meet with sufficient regularity so it can properly discharge its duties and responsibilities and carry out its functions in relation to the regulated entity.

6.8 Minutes of board and board committee meetings

The board of a regulated entity shall ensure that the regulated entity keeps minutes and associated documents of all of its board and board committee meetings. These shall provide an adequate and appropriate record of corresponding proceedings including, but not limited to, all material considerations, decisions and actions.

Those minutes shall —

(a) without undue delay after the meeting to which they relate, be written up and distributed in final draft to all persons entitled to receive a copy; and

(b) within a reasonable timeframe, be accepted by the board (or, if a committee meeting, the committee) and signed as a formal record of the meeting by a duly authorised person.

7. KEY FUNCTIONS AND RESPONSIBILITIES OF THE BOARD

7.1 Ultimate accountability and responsibility, and delegation

(a) The board of a regulated entity is ultimately accountable and responsible for the affairs of the regulated entity. Delegating authority to board committees, management or others does not absolve the board of its duties and responsibilities in relation to the regulated entity.

(b) Where the board of a regulated entity delegates any of its functions in relation to the regulated entity, it shall only do so in a manner that does not —

(i) dilute its ultimate accountability in relation to the regulated entity;

(ii) reduce its ability to discharge properly its duties and responsibilities or carry out its functions in relation to the regulated entity; or

(iii) lead to any person having unfettered powers in relation to the regulated entity.

(c) The board of a regulated entity shall ensure that any authority it has delegated to carry out a function in relation to the regulated entity is properly authorised, communicated and documented.

(d) Notwithstanding any delegation, the board of a regulated entity shall provide sound and prudent oversight in relation to the regulated entity's affairs. Accordingly it shall —

(i) ensure it receives timely, accurate, relevant and sufficiently comprehensive information and analyses relating to the regulated entity, its management and external environment such that it can properly discharge its duties and responsibilities and carry out its functions in relation to the regulated entity;

(ii) ensure that the regulated entity has taken all reasonable steps to identify and comply with its legal and regulatory obligations in accordance with paragraph 5.2;

(iii) satisfy itself that the strategies and significant policies and procedures it has established in relation to the regulated entity have been properly implemented and are being adhered to; and

(iv) satisfy itself that any authority it has delegated in relation to the regulated entity has been responsibly and prudently exercised, and such authority has not been exceeded.

7.2 Identification of responsibilities, authority and accountabilities

The board of a regulated entity shall —

(a) establish and maintain, and distinguish between, the responsibilities, decision-making, interaction and cooperation of the regulated entity's —

(i) board;

(ii) where established, board committees;

(iii) where appointed, chairman and chief executive (or equivalent);

(iv) senior management; and

(v) any outsourced provider of a significant function of the regulated entity;

(b) establish and maintain decision-making processes and divisions of responsibility that ensure an appropriate balance of power and authority for the regulated entity, so that —

(i) no person has unfettered powers of decision in relation to the regulated entity; and

(ii) contractual arrangements and other transactions of the regulated entity are only entered into with appropriate authority; and

(c) satisfy itself that the regulated entity is organised and controlled in a way that provides for its sound and prudent management including, but not limited to, accountability to the board and proper oversight by the board of its board committees, senior management and any outsourced provider of a significant function of the regulated entity.

7.3 Board committees

The board of a regulated entity shall assess the need for and, where appropriate, establish committees of the board.

Where such a committee is established, the board shall —

(a) define adequate and appropriate terms of reference of the committee and these shall set out the committee's purpose, responsibilities, authority, composition and the means by which the committee is monitored and held accountable to the board;

(b) ensure that the committee is composed of persons with the appropriate combined level of knowledge, skills, experience and commitment for the committee's role in relation to the regulated entity; and

(c) ensure that the committee's terms of reference are in writing and are made available to relevant parties, including, but not limited to, the regulated entity's senior management (where appropriate) and external auditor.

7.4 Directors and senior management

The board of a regulated entity shall —

(a) establish the means by which the regulated entity's senior management is monitored and held accountable to the board;

(b) subject to paragraph (c) insofar as its powers permit,

(i) approve the selection, appointment, removal and any applicable succession planning of the regulated entity's directors and senior management; and

(ii) ensure that the regulated entity's individual directors and senior managers possess the appropriate integrity, competence, experience and qualifications for their respective roles in relation to the regulated entity; and

(c) where the regulated entity's senior management is outsourced to an insurance manager registered under section 25 of the Act, paragraph 7.5 shall apply instead of paragraph (b).

7.5 Outsourced providers of significant outsourced functions

The board of a regulated entity shall —

(a) ensure that the arrangements for any outsourced significant function of the regulated entity are consistent with paragraph 10; and

(b) approve the selection, appointment, removal and any applicable succession planning of any outsourced provider of a significant function of the regulated entity.

7.6 Governance principles

The board of a regulated entity shall —

(a) establish and maintain specific corporate governance principles in respect of the regulated entity that are adequate and appropriate to the nature, scale and complexity of the regulated entity, its activities and the risks to which it is exposed; and

(b) ensure that the strategies, significant policies and other systems of governance established by the board in relation to the regulated entity have due regard for, and are consistent with, those principles.

7.7 Standards of conduct

The board of a regulated entity shall establish and maintain policies defining standards of business conduct for its directors, senior managers, employees, and any outsourced providers of a significant function of the regulated entity, that address in an adequate and appropriate manner —

(a) conflicts of duty or interest in relation to the regulated entity;

(b) matters in relation to the regulated entity involving private transactions, self-dealing, preferential treatment of favoured internal and external parties, covering trading losses and any other practices of a potentially non-arm's length nature; and

(c) the fair treatment of, and information sharing with, the regulated entity's stakeholders.

7.8 Strategies, significant policies and business plans

The board of a regulated entity shall —

(a) establish and maintain adequate and appropriate strategies and significant policies in relation to the regulated entity for all of its significant business decision areas;

(b) establish and maintain the means of pursuing those strategies and adhering to those policies;

(c) review and approve the significant business plans of the regulated entity;

(d) evaluate at appropriate intervals, and at least annually, the regulated entity's performance against those business plans in light of those strategies and policies; and

(e) review the strategies and significant policies of the regulated entity at appropriate intervals, and at least annually, and adapt them as necessary to ensure they remain adequate, appropriate and effective in relation to the regulated entity and its external environment.

7.9 Remuneration

The board of a regulated entity shall establish and maintain a remuneration policy for its directors, senior managers and employees as well as any outsourced provider of a significant function of the regulated entity.

That policy, together with any relevant internal controls, shall ensure that corresponding remuneration is consistent with the effective risk management of the regulated entity such that imprudent or improper behaviour is not encouraged.

7.10 Financial reporting system

The board of a regulated entity shall establish and maintain a system for the regulated entity's financial reporting that ensures the integrity, reliability and transparency of that reporting both for public, where applicable, and regulatory purposes.

7.11 Information and communication systems

The board of a regulated entity shall establish and maintain information and other communication systems in relation to the regulated entity which —

(a) are reliable;

(b) ensure the prompt and effective transfer of information between —

(i) all levels of management within the regulated entity;

(ii) the regulated entity and any outsourced provider of a significant function of the regulated entity; and

(iii) the regulated entity and its stakeholders; and

(c) are secure such that the regulated entity's information is safeguarded.

7.12 Risk management and financial management

The board of a regulated entity shall —

(a) establish and maintain a risk management system for the regulated entity that is consistent with paragraph 15;

(b) allocate responsibility for, and ensure it receives, risk management reports in accordance with paragraph 15.3;

(c) establish and maintain the risk strategies and significant risk policies and procedures of the regulated entity including, but not limited to, appropriate risk tolerance limits in respect of all material sources of risk to which it is exposed;

(d) review at appropriate intervals, and at least annually, the regulated entity's risk profile; and

(e) coordinate the risk management and financial management of the regulated entity to ensure that the capital and other financial resources of the regulated entity are managed in accordance with paragraph 5.5.

7.13 Internal control framework

The board of a regulated entity shall, as part of the regulated entity's risk management system —

(a) establish and maintain an internal control framework for the regulated entity that is consistent with paragraph 16;

(b) allocate responsibility for, and ensure it receives, reports in accordance with paragraphs 12.3 and 13.4 as applicable to the regulated entity;

(c) ensure timely action is taken, where necessary, to correct any identified —

(i) weaknesses or deficiencies in the regulated entity's internal controls, procedures or other systems of governance;

(ii) material instances of non-compliance with the regulated entity's internal policies or procedures; and

(iii) non-compliance with the regulated entity's legal or regulatory obligations; and

(d) review at appropriate intervals, and at least annually, the regulated entity's material —

(i) internal controls;

(ii) procedures; and

(iii) other systems of governance,

in a manner that is consistent with paragraph 12, to ensure they remain adequate, appropriate and effective (and, for the avoidance of doubt, in undertaking such a review the board may place reasonable reliance upon any internal audit or compliance function work it has delegated).

7.14 Other arrangements

The board of a regulated entity shall ensure that the regulated entity has in place arrangements for —

(a) fraud prevention in accordance with paragraph 17;

(b) whistle blowing in accordance with paragraph 18;

(c) fair treatment of policyholders in accordance with paragraph 19 (as applicable); and

(d) interaction with the Supervisor in accordance with paragraph 20.

7.15 Culture

The board of a regulated entity shall promote a culture throughout the regulated entity that supports the —

(a) corporate governance principles established by the board in relation to the regulated entity;

(b) ongoing and effective risk management and financial management, and compliance, of the regulated entity; and

(c) fair treatment of the regulated entity's stakeholders.

7.16 Self assessment

The board of a regulated entity shall at appropriate intervals, and at least annually, evaluate its own composition (as referred to in paragraph 6.2(a)) and performance, and implement remedial measures as necessary to address any identified inadequacies in its ability or performance in discharging its duties and responsibilities or carrying out its functions in relation to the regulated entity.

8. KEY RESPONSIBILITIES OF DIRECTORS

A director of a regulated entity shall —

(a) act on a well informed basis, in good faith, with due care, skill and diligence, with integrity and in the best interests of the regulated entity;

(b) have due regard for the interests of the regulated entity's stakeholders in his decision making;

(c) identify and either avoid or promptly disclose to the board of the regulated entity any conflicts of duty or interest he has or may have in relation to the regulated entity;

(d) be free from any undue influence in exercising his judgement in respect of the regulated entity;

(e) ensure he has the appropriate integrity, competence, experience, qualifications and commitment so he can properly discharge his duties and

responsibilities and carry out his functions in relation to the regulated entity; and

(f) properly discharge his duties and responsibilities and carry out his functions in relation to the regulated entity.

9. KEY RESPONSIBILITIES OF SENIOR MANAGEMENT

The senior management of a regulated entity shall —

(a) establish, implement and maintain internal controls and procedures to ensure the sound and prudent management of the regulated entity within —

(i) the strategies and policies of the regulated entity established by its board; and

(ii) the regulated entity's legal and regulatory obligations as identified in accordance with paragraph 5.2;

(b) manage the day to day operations of the regulated entity, ensuring those operations are carried out in accordance with the regulated entity's —

(i) strategies, policies and procedures established by its board; and

(ii) legal and regulatory obligations as identified in accordance with paragraph 5.2;

(c) promote a culture throughout the regulated entity that supports the —

(i) regulated entity's corporate governance principles established by its board;

(ii) ongoing and effective risk management and financial management, and compliance, of the regulated entity; and

(iii) fair treatment of the regulated entity's stakeholders;

(d) individually identify and either avoid or promptly disclose to the board of the regulated entity any conflicts of duty or interest he has or may have in relation to the regulated entity;

(e) provide to the regulated entity's board such risk management reports as the board may specify in relation to the requirements of paragraph 15.3;

(f) provide the regulated entity's board with timely, accurate, relevant, and sufficiently comprehensive information to enable the board to review —

(i) the regulated entity's performance and the performance of its senior management;

(ii) the regulated entity's business strategy and policies established by the board in relation to the regulated entity; and

(iii) such other matters in relation to the regulated entity as the board may specify; and

(g) provide the regulated entity's board with recommendations, as appropriate, for its review and approval on the strategy, significant policies and business plans that govern the operation of the insurer.

10. OUTSOURCED SIGNIFICANT FUNCTIONS

Where a significant function of a regulated entity has been outsourced, the regulated entity shall ensure that —

(a) where the outsourced provider is required to have any regulatory consents in order to carry out the outsourced function, those consents have been obtained and remain in force;

(b) the outsourced provider has the appropriate integrity, competence, experience and qualifications to carry out the outsourced function;

(c) the outsourced provider has the capacity to carry out the outsourced function taking into account the size and timing of corresponding workloads;

(d) its use of the outsourced provider is consistent with the —

(i) ongoing and effective risk management and financial management, and compliance, of the regulated entity;

(ii) standard of control that would apply if the outsourced function was carried out internally by the regulated entity;

(iii) fair treatment of the regulated entity's stakeholders (as applicable);

(iv) effective operation of the external audit of the regulated entity; and

(v) ongoing, open, honest and timely communication with the Supervisor in relation to the activities of the regulated entity; and

(e) a written agreement is in place with the outsourced provider, where the board of the regulated entity understands and authorises the terms and conditions of that agreement, and that agreement —

(i) is binding on both parties;

(ii) sets out clearly the rights, expectations and obligations of both parties;

(iii) provides for the termination and orderly winding up of the outsourced arrangement; and

(iv) includes the means by which the outsourced provider is monitored and held accountable to the regulated entity in relation to the outsourced function.

11. ACTUARY

11.1 Operational requirements

Where an insurer has appointed an actuary, the insurer shall —

(a) insofar as it is necessary for the performance of the actuary's function in relation to the insurer, afford the actuary the right of direct access at all reasonable times to —

(i) the board,

(ii) the directors, senior management and other employees and functions; and

(iii) any outsourced provider of a significant function;

(iv) the external auditor; and

(v) all information and data,

of the insurer; and

(b) require the actuary, within the terms of the actuary's appointment in relation to the insurer, to report to the board of the insurer on a timely basis on matters relevant to that appointment.

11.2 Objective judgement

In forming and formulating his own actuarial opinion or advice, the actuary of an insurer shall be objective and free from any undue influence (for example, from other functions, directors, management or other employees of the insurer) and provide his opinions and advice to the board and Supervisor (as applicable) in an independent manner.

11.3 Dual role of appointed actuary and director

The positions of actuary and director shall not be combined in one individual within the same insurer where that insurer is carrying on class 2 business or where such combining of roles would otherwise be likely to result in a material conflict.

Where the posts of actuary and director are combined, the insurer's board shall —

(a) establish and maintain adequate and appropriate internal controls to ensure that the actuary remains objective and free from any undue influence such that his opinions and advice to the board and Supervisor (as applicable) are provided in an independent manner; and

(b) at appropriate intervals, and at least annually, review —

(i) the reasons for combining the posts of actuary and director to ensure they remain valid; and

(ii) the internal controls established under paragraph (a) to ensure they remain adequate, appropriate and effective.

12. INTERNAL AUDIT FUNCTION

12.1 Meaning of "internal audit function" in the CGC

The internal audit function of an insurer is the means applied by the insurer's board to objectively examine and evaluate the —

(a) insurer's material —

(i) internal controls;

(ii) procedures; and

(iii) other systems of governance,

to ensure they are adequate, appropriate and effective for the insurer, its activities and the risks to which it is exposed; and

(b) compliance of the insurer's activities with its internal strategies, policies and procedures, as well as its legal and regulatory obligations as identified in accordance with paragraph 5.2.

12.2 General

An insurer shall have an ongoing and effective internal audit function that is adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is exposed.

Accordingly, an insurer shall ensure that its internal audit function —

(a) has appropriate independence from the operational activities it audits;

(b) has direct reporting lines to the insurer's board;

(c) has sufficient status within the insurer to ensure that the directors and senior management of the insurer react appropriately to its enquiries and recommendations;

(d) has unrestricted access at all reasonable times to —

(i) the board,

(ii) directors, senior management and other employees and functions;

(iii) any outsourced provider of a significant function;

(iv) the external auditor; and

(v) all information and data,

of the insurer, as is necessary for the performance of its activities in relation to the insurer;

(e) has sufficient resources and utilises individuals that are suitably trained and have relevant experience to understand and evaluate effectively the insurer's business and risks that those individuals are involved in auditing;

(f) employs a methodology that identifies the material risks to which the insurer is exposed and allocates its resources accordingly; and

(g) encompasses both internal and any outsourced functions of the insurer.

12.3 Reporting and recording

The findings and recommendations of an insurer's internal audit function shall be reported in writing at appropriate intervals, and at least annually, to the insurer's board.

Those reports shall detail at least any identified —

(a) significant weaknesses within the insurer's internal controls, procedures or other systems of governance;

(b) material instances of non-compliance with the insurer's internal policies or procedures;

(c) non-compliance with the insurer's legal or regulatory obligations; and

(d) failures to deal properly with past recommendations of the internal audit function,

and, in respect of each of the paragraphs (a) to (d), the reports shall either make remedial recommendations as may be necessary or shall include a statement in each case that no such matters have been identified.

Where the board carries out the internal audit function itself, it need not prepare such a report but shall keep an adequate and appropriate record of its equivalent findings and decisions.

12.4 Delegation (including outsourcing)

Without limiting any of paragraphs 12.1 to 12.3, the board of an insurer may carry out the insurer's internal audit function itself or may delegate it fully or in part to one or more other resources, including —

(a) a committee of the board;

(b) a suitable resource from within the insurer;

(c) where the insurer is part of a group, its group's internal audit function or other suitable resource from within its group;

(d) where the insurer has an appointed insurance manager, the internal audit function of the insurance manager or other suitable resource from within the insurance manager or, where the insurance manager is part of a group, that group's internal audit function or other suitable resource from within that group; or

(e) a suitable external party.

13. COMPLIANCE FUNCTION

13.1 Meaning of "compliance function" in the CGC

The compliance function of a regulated entity is the means applied by the regulated entity to —

(a) identify and understand the regulated entity's legal and regulatory obligations in accordance with paragraph 5.2; and

(b) establish, implement and maintain compliance strategies, policies, procedures and training,

in order to ensure that the regulated entity complies with its legal and regulatory obligations as identified in accordance with in paragraph 5.2.

13.2 General

A regulated entity shall have an ongoing and effective compliance function that is adequate and appropriate to the nature, scale and complexity of the regulated entity, its activities and the risks to which it is exposed.

This includes the compliance function having adequate and appropriate expertise, resources and authority to carry out its activities effectively.

13.3 Nature and location

Without limiting paragraph 13.1 or 13.2, the compliance function of a regulated entity —

(a) may be carried out internally by the regulated entity or by a suitable external party or a combination of both;

(b) shall be ultimately controlled in or from the Isle of Man; and

(c) subject to paragraph (d), shall be substantially carried out in or from the Isle of Man; or

(d) where operational functions of the regulated entity are carried out outside of the Isle of Man, the regulated entity's corresponding compliance function may be carried out by parties that are either located in the Isle of Man or located outside of the Isle of Man.

For the avoidance of doubt, this paragraph does not restrict a regulated entity from obtaining advice from outside of the Isle of Man as appropriate to its activities.

13.4 Reporting

The compliance function of a regulated entity shall report at appropriate intervals, and at least annually, to the regulated entity's board on compliance matters in accordance with its role in relation to the regulated entity.

14. EXTERNAL AUDIT

14.1 General

A regulated entity shall —

(a) take all reasonable steps to ensure it affords its external auditor all of the rights and entitlements applicable to the position of external auditor; and

(b) permit and not deter its external auditor from providing to the Supervisor such information and confirmations as the Supervisor requests for the purposes of carrying out of the functions of the Supervisor.

14.2 Engagement letter

Prior to commencement of its audit, a regulated entity shall obtain from its external auditor a letter of engagement which —

(a) contains an undertaking of the external auditor to provide to the regulated entity, and upon request to the Supervisor, the governance communications referred to in paragraph 14.3;

(b) defines clearly the extent of the rights and duties of the external auditor; and

(c) is signed and accepted in writing by both parties.

14.3 Governance communication

A regulated entity shall at the same time as its annual accounts are submitted to the Supervisor —

(a) provide to the Supervisor a copy of the communication, in relation to those accounts, made by its external auditor to those charged with the regulated entity's governance pursuant to International Standard on Auditing 260 ("ISA 260") or International Standard on Auditing (UK and Ireland) 260 ("ISA (UK and Ireland) 260"), or equivalent;

(b) inform the Supervisor whether the regulated entity has implemented or is in the process of implementing the recommendations, or has addressed or is in the process of addressing the weaknesses, identified (if any) in that communication, or, if not, provide its reasons for not doing so; and

(c) where the regulated entity receives no ISA 260 or ISA (UK and Ireland) 260 communication, or equivalent, provide the Supervisor with a copy of its external auditor's confirmation that no such communication has been or is anticipated to be issued.

A regulated entity shall, without undue delay, provide to the Supervisor a copy of any other formal communication it receives from its external auditor that identifies any material weakness relating to the regulated entity's internal controls, procedures or other systems of governance.

15. RISK MANAGEMENT SYSTEM

15.1 General

A regulated entity shall —

(a) establish, implement and maintain an effective risk management system that is adequate and appropriate to the nature, scale and complexity of the regulated entity, its activities and the risks to which it is exposed, and is —

(i) consistent with paragraph 15.2; and

(ii) able to report in accordance with paragraph 15.3;

(b) maintain a thorough understanding of its risk profile, including the types, characteristics, interdependencies, sources and potential impact of those risks on an individual and aggregate basis; and

(c) integrate its risk management system into its decision making processes so that decisions can be taken with due regard for the risks involved.

15.2 System

The risk management system of a regulated entity shall —

(a) be ongoing and comprehensive including, but not limited to, strategies, policies, and procedures that promptly and effectively —

(i) identify, assess and measure;

(ii) monitor and control; and

(iii) where appropriate, mitigate;

all reasonably foreseeable, material risks to which the regulated entity is exposed;

(b) encompass all relevant risks on an individual and aggregate basis including, but not limited to, the risks referred to in Schedule 1 – as applicable to the regulated entity; and

(c) ensure that the operations and risk exposures of the regulated entity are within the risk tolerance limits established by its board in respect of the regulated entity in accordance with paragraph 7.12(c).

15.3 Reporting

The board of a regulated entity shall ensure it receives at appropriate intervals, and at least annually, risk management reports and all other relevant information that will enable it to adequately and effectively —

(a) oversee the regulated entity's risk management system;

(b) review its risk profile; and

(c) assess the adequacy of its capital and other financial resources in accordance with paragraphs 5.5(a) and 5.5(b).

16. INTERNAL CONTROL FRAMEWORK

16.1 Framework

The internal control framework of a regulated entity is part of its risk management system and includes its —

(a) internal audit function as referred to in paragraph 12 (as applicable);

(b) compliance function as referred to in paragraph 13; and

(c) internal controls as referred to in paragraph 16.2.

A regulated entity's internal control framework shall also have due regard for the findings and recommendations communicated to the regulated entity by its actuary (where applicable), and its external auditor.

16.2 Internal controls

A regulated entity shall establish, implement and maintain effective internal controls including, but not limited to —

(a) arrangements for delegating authority and segregation of duties; and

(b) other checks and balances,

that are adequate and appropriate to the nature, scale and complexity of the regulated entity, its activities and the risks to which it is exposed to ensure that the regulated entity and other persons (as applicable) adhere to the —

(i) regulated entity's strategies, policies and procedures established by its board;

(ii) requirements of the CGC; and

(iii) regulated entity's other legal and regulatory obligations as identified in accordance with paragraph 5.2.

For the avoidance of doubt, this paragraph does not limit any other requirement in relation to internal controls or procedures included elsewhere within the CGC.

17. FRAUD PREVENTION

A regulated entity shall ensure that high standards of integrity apply to all aspects of its business, and shall —

(a) establish, implement and maintain adequate and appropriate internal controls and procedures to deter, detect, record and as required promptly report any fraud it becomes aware of to the appropriate authorities;

(b) assign operational responsibility for the regulated entity's fraud prevention and reporting to suitably senior officers or employees of the regulated entity;

(c) take adequate and appropriate measures to prevent fraud, including, but not limited to, providing counter-fraud training to its directors, senior managers and employees; and

(d) ensure that the internal controls and procedures, as referred to in paragraph (a), form an integral part of the regulated entity's risk management system.

18. WHISTLE BLOWING

A regulated entity shall establish, implement and maintain an adequate and appropriate policy and procedures to encourage the reporting of any improper or unlawful behaviour, which shall —

(a) define the scope of improper or unlawful behaviour covered by the policy, including but not limited to —

(i) failure to comply with the regulated entity's legal and regulatory obligations;

(ii) financial malpractice or fraud;

(iii) criminal activity;

(iv) improper conduct or unethical behaviour; and

(v) attempts to conceal any malpractice or fraud;

(b) set out a reporting structure to enable the regulated entity's directors, senior managers and employees to raise concerns outside of the normal management reporting structure;

(c) state how, and ensure that, matters so reported are considered objectively and that appropriate and timely actions are taken;

(d) adequately and appropriately protect the whistleblower from any negative repercussions arising from reporting in good faith their concerns, including, but not limited to, ensuring confidentiality; and

(e) be communicated effectively to all relevant persons to whom it applies.

19. FAIR TREATMENT OF POLICYHOLDERS

19.1 Policyholders

An insurer shall establish, implement and maintain policies on how to treat its policyholders fairly, as well as adequate and appropriate internal controls and procedures, including training where necessary, to ensure compliance with those policies by the insurer's directors, senior managers, employees and other persons appointed to act on behalf of the insurer. This includes, but is not limited to —

(a) where the insurer, or a person appointed to act on behalf of the insurer, is dealing directly with its policyholders, ensuring that information is sought from the policyholder that is appropriate in order to assess the policyholder's relevant needs before giving advice or concluding a contract;

(b) ensuring that all reasonable steps are taken in a timely manner to enable its policyholders to take suitably informed decisions by providing adequate and appropriate information to the policyholder, or relevant person appointed to act on behalf of the policyholder, concerning the insurer's product applicable to the policyholder, including, but not limited to —

(i) the product's risks, benefits, obligations and charges; and

(ii) timely disclosure to the policyholder of any conflict of duty or interest on the part of the insurer's directors, senior managers,

employees or other persons appointed to act on behalf of the insurer that is relevant to the sale of the product;

(c) ensuring clear and effective communication with its policyholders and avoiding any false, misleading or deceptive representations or practices either by itself or knowingly on its behalf;

(d) ensuring that the insurer deals with claims and complaints effectively and fairly through an easily understood, well disclosed, easily accessible and equitable process; and

(e) ensuring, in the event of a complaint, that adequate, appropriate and timely information is provided to the complainant in respect of the Isle of Man Financial Services Ombudsman Scheme.

19.2 Member policyholders and participating policyholders

Where an insurer has member policyholders or participating policyholders it shall establish, implement and maintain policies and procedures to ensure that any rights and entitlements of those policyholders are treated by the insurer in a fair and equitable manner.

20. INTERACTION WITH THE SUPERVISOR

A regulated entity shall —

(a) maintain open, honest and timely communications with the Supervisor, including communicating with the Supervisor as required and meeting with the Supervisor when requested;

(b) maintain open, honest and timely communications with any other regulatory body to which it is accountable; and

(c) establish, implement and maintain adequate and appropriate internal controls to ensure the accuracy and timeliness of any information it provides to the Supervisor and any other regulatory body to which the regulated entity is accountable.

21. INTERPRETATION

In the CGC —

"the Act" means the Insurance Act 2008;

"actuary", in relation to an insurer, means the person appointed as actuary to the insurer in accordance with section 18 of the Act;

"annual accounts" in relation to —

(a) an insurer has the meaning as given in section 54 of the Act; and

(b) an insurance manager registered under section 25 of the Act means —

(i) the profit and loss account for the financial period or, in the case of an insurance manager not trading for profit, an income and expenditure account for the period; and

(ii) the balance sheet as at the end of the financial period,

prepared in accordance with the provisions of the Partnership Act 1909, the Companies Acts 1931 to 2004, the Limited Liability Companies Act 1996 or the Companies Act 2006 relating to accounts (as applicable), and in accordance with requirements imposed by the Supervisor under the Act;

"asset-liability management", in relation to a regulated entity, refers to the practice of managing its assets and liabilities so that decisions and actions taken in respect of those assets and liabilities are coordinated in order to manage the regulated entity's corresponding risk exposures;

"board", in relation to a regulated entity, means the board of directors of the regulated entity or, where the regulated entity has no board of directors, its equivalent governing body;

"business plans", in relation to a regulated entity, mean the detailed activity plans and financial projections of the material operations of the regulated entity;

"**the CGC"** means these Guidance Notes, titled the Corporate Governance Code of Practice for Regulated Insurance Entities;

"class 2 business" has the meaning as given in regulation 2 of the Insurance Regulations 1986;

"compliance function" has the meaning as given in paragraph 13.1;

"constitutional documents", in relation to a regulated entity, mean its memorandum and articles of association, or their equivalent, and any other formal document of the regulated entity that establishes the existence of the regulated entity or regulates its structure, control or members;

"**derivative"** means a financial asset or liability whose value depends on, or is derived from, other underlying factors, such as, but not limited to —

(a) assets;

(b) liabilities;

(c) interest rates;

(d) currency exchange rates; or

(e) indices,

and includes, but is not limited to, forwards, futures, options, warrants, swaps, and other financial instruments that have a similar economic effect;

"dormant", in relation to a regulated entity, has the meaning as given in section 12A(3) of the Companies Act 1982, and includes that the regulated entity has no current or residual insurance exposure;

"front office", in relation to an insurer, refers to those functions of the insurer that come in direct contact with its policyholders;

"group", in relation to a regulated entity, means—

(a) the regulated entity,

(b) any other legal person which is —

(i) its subsidiary;

(ii) its holding company; or

(iii) a subsidiary of that holding company;

"holding company" shall be construed in accordance with the definition of subsidiary;

"independent non-executive director", in relation to a regulated entity, means a director of the regulated entity who —

(a) apart from his —

(i) directors' fees in respect of his position as a director of the regulated entity; and

(ii) subject to paragraph (b) —

1. other benefits attributable to his position as a director of the regulated entity; and

2. shareholdings in relation to the regulated entity or its group,

as may be applicable, is independent of the group (as applicable) and management of the regulated entity; and

(b) is free from any relationships or circumstances which could materially interfere with the exercise of his independent judgment in relation to the affairs of the regulated entity;

"insurance provisions" —

(a) in relation to the insurance business other than long-term business of an insurer, are the amounts set aside as liabilities on the insurer's balance sheet to meet its obligations arising out of its insurance contracts as well as related expenses (including, but not limited to, as applicable: provisions for claims, claims incurred but not reported, claims incurred but not enough reported, unearned premium, unexpired risk and policyholder profit participation); and

(b) in respect of the long-term business of an insurer, are the amounts set aside to meet its obligations arising out of its long-term insurance contracts in accordance with the Insurance (Valuation of Long Term Liabilities) Regulations 2007;

"insurer" means a person authorised under section 8 of the Act or permitted under section 22 of the Act;

"internal audit function" has the meaning as given in paragraph 12.1;

"member policyholder", in relation to an insurer that is a mutual (or equivalent), is a member of the mutual (or equivalent) who is also insured by the insurer (either directly or by way of reinsurance);

"outsourced function", in relation to a regulated entity, refers to a function of the regulated entity that is carried out by a person external to the regulated entity;

"outsourced provider", in relation to a regulated entity, refers to a person external to the regulated entity (whether within or external to the regulated entity's group) that carries out an outsourced function of the regulated entity;

"participating policyholder", in relation to an insurer, is a policyholder of the insurer whose policy with the insurer, in addition to any right to be indemnified under that policy, gives the policyholder a right to participate in the profits of the insurer;

"policyholder" has the meaning as given in section 54 of the Act and, where appearing, also includes prospective policyholders of the insurer as the context requires;

"regulated entity" means a person to whom the CGC applies in accordance with paragraph 3.1;

"risk profile", in relation to a regulated entity, means the particular range and significance of risks to which the regulated entity is exposed;

"risk tolerance limits", in respect of a regulated entity, mean policy statements established by its board specifying the nature and amount of risk exposure the regulated entity is willing to accept and not exceed;

"senior management", in relation to a regulated entity, means any person whose appointment is required to be notified to the Supervisor under the Act, excluding its —

(a) non-executive directors;

(b) external auditor; and

(c) controllers where such a controller is not a person whose appointment is required to be notified to the Supervisor under the Act other than as a controller;

"senior manager", in relation to a regulated entity, means a member of its senior management;

"shareholders", in relation to a regulated entity, mean the owners of the regulated entity including (as applicable) —

(a) the owners of its shares;

(b) its members (if the regulated entity is a mutual or similar);

(c) its partners (if the regulated entity is a partnership); and

(d) in the case of an insurer, its member policyholders and participating policyholders,

or their equivalents;

"stakeholder", in relation to a regulated entity, means any person with a direct or indirect interest or involvement (a stake) in the regulated entity because that person can affect or be affected by the regulated entity's actions, strategies, policies or procedures (a regulated entity's stakeholders include, but are not limited to, where applicable, its policyholders, shareholders and other investors, creditors, employees, the general public, the Isle of Man Government and the Insurance and Pensions Authority); and

"**subsidiary**" means a legal person (whether or not incorporate under the Companies Acts 1931 to 2004) that is a subsidiary of another legal person (whether or not incorporated under those Acts) and in determining whether one legal person is a subsidiary of another the provisions of section 1 of the Companies Act 1974 shall

apply with the necessary modifications, and "holding company" shall be construed accordingly.

22. SCHEDULES

The Schedules listed below form part of the CGC's binding guidance.

22.1 Schedule 1 – Risks

22.2 Schedule 2 – Directors' Certificate on Corporate Governance

Paragraphs 15.2(b) and 22.1

SCHEDULE 1

RISKS

Without limiting the CGC's other guidance, a regulated entity shall apply the guidance within this Schedule as is applicable to the regulated entity.

The risks referred to in this Schedule are not intended to be, and shall not be interpreted as being, exhaustive.

The order in which the risks appear, and the extent to which guidance is or is not given, in this Schedule does not attach any greater or lesser significance to any particular risk.

Underwriting risk

Underwriting risk, in relation to an insurer, refers to the risks arising out of its day to day activities in underwriting contracts of insurance, as well as risks associated with its outward reinsurance and any other risk transfer, mitigation or diversification mechanism relevant to its underwriting strategy.

In managing this risk an insurer shall apply the following guidance:

(a) An insurer shall establish, implement and maintain strategic underwriting and pricing policies based on sound methodology and reasonable assumptions that are approved, monitored and reviewed by its board.

(b) An insurer shall evaluate prudently the risks it underwrites and establish, implement and maintain an adequate level of premiums for those risks that will enable the insurer to meet all of its reasonably foreseeable claims and other obligations arising out of its underwriting activities, and related expenses.

(c) An insurer shall establish, implement and maintain systems to control all of the claims and other obligations and expenses referred to in paragraph (b), and those systems shall be monitored on an ongoing basis by its senior management and properly overseen by its board.

(d) An insurer shall have a clear strategy to mitigate, and where appropriate diversify, the underwriting risks to which it is exposed by defining limits on the amount of risk it retains and (where applicable) taking out appropriate reinsurance cover, or using other risk transfer arrangements, consistent with it maintaining adequate capital and other financial resources in accordance with paragraphs 5.5(a) and 5.5(b). This strategy shall be an integral part of

the insurer's underwriting policy that is approved, monitored and reviewed by its board.

(e) An insurer shall ensure that its outwards reinsurance arrangements (where applicable) are adequate and that the claims held by the insurer against its reinsurers are recoverable, this includes —

(i) ensuring that its reinsurance programme is appropriate to its risk profile and provides coverage which, after taking into account the the real transfer of risk, enables the insurer to maintain adequate capital and other financial resources in accordance with paragraphs 5.5(a) and 5.5(b); and

(ii) taking all reasonable steps to ensure that the protection provided by its reinsurers is secure.

(f) In addition to paragraph (e), an insurer shall ensure that any other risk transfer mechanism it uses provides adequate protection which, after taking into account the ultimate collectability of inward amounts to the insurer and the real transfer of risk, enables the insurer to maintain adequate capital and other financial resources in accordance with paragraphs 5.5(a) and 5.5(b).

(g) An insurer shall ensure that all of its risk transfer mechanisms are properly accounted for so that the insurer's financial statements give a true and fair view of the insurer's risk exposure.

Insurance provisions risk

To avoid doubt, the following guidance in relation to insurance provisions risk does not limit the Insurance (Valuation of Long Term Liabilities) Regulations 2007.

Insurance provisions risk, in relation to an insurer, refers to the possibility that the insurer's insurance provisions prove to be inadequate to encompass all of the insurer's obligations arising out of its insurance contracts as well as related expenses.

In managing this risk an insurer shall apply the following guidance:

(a) An insurer shall identify and quantify prudently its existing and anticipated obligations arising out of its insurance contracts as well as related expenses.

(b) An insurer shall, after making reasonable allowance for its corresponding reinsurance amounts recoverable (or other relevant risk transfer mechanism), establish and maintain adequate insurance provisions to meet the total cost of claims and other obligations of the insurer arising out of its insurance contracts, as well as related expenses, including all reasonably foreseeable —

(i) claims incurred, and claims not yet incurred, by the insurer; and

(ii) related administration expenses, policyholder dividends and bonuses, taxes, expenses relating to embedded options, and any other attributable costs to the insurer.

(c) An insurer's insurance provisions shall be based on —

(i) sound accounting and, where appropriate, actuarial principles that are appropriate for insurance companies and the types of business undertaken by the insurer;

(ii) reliable data; and

(iii) appropriate methods and assumptions for assessing on a reliable, objective, transparent and prudent basis, insurance provisions for the types of business undertaken by the insurer.

(d) An insurer's policy for establishing and maintaining its insurance provisions shall, amongst other things, take into account the potential for unexpected or atypical claims (and other expenses) occurrence and catastrophe events that might adversely affect the insurer. This includes, but is not limited to, where appropriate, undertaking regular stress testing (as part of the requirement under paragraph 5.5(c)) for an appropriate range of adverse scenarios in order to assess the adequacy of its capital and other financial resources in accordance with paragraphs 5.5(a) and 5.5(b), such that should its insurance provisions need to be increased it has sufficient capital and other financial resources to do so.

Investment risk

Investment risk, in relation to a regulated entity, encompasses the various risks to which the regulated entity is exposed in relation to its investment activities.

Investment risks may include, but are not limited to, credit risk, market risk, liquidity risk and custody risk. These and other component risks are described further in this schedule.

In managing this risk a regulated entity shall apply the following guidance:

(a) A regulated entity shall establish, implement and maintain an overall strategic investment policy that addresses the following elements (as applicable) —

(i) the regulated entity's risk profile;

(ii) the regulated entity's asset-liability management policies;

(iii) the regulated entity's other risk management policies;

(iv) the determination of the strategic asset allocation, that is, the long-term asset mix over the main investment categories;

(v) the establishment of limits for asset allocation by geographical area, markets, sectors, counterparties and currency;

(vi) the extent to which the holding of some types of assets is restricted or disallowed;

(vii) the conditions under which the regulated entity can pledge or lend assets;

(viii) limits of delegated authority to make or alter the regulated entity's investments;

(ix) clear accountability in respect of all of its asset transactions and associated risks; and

(x) where the regulated entity is using or intending to use derivatives, an overall policy on their use.

(b) An insurer's risk management system shall, amongst other things, cover the risks associated with its investment activities that might affect the coverage of its insurance provisions or maintaining adequate capital and other financial resources in accordance with paragraphs 5.5(a) and 5.5(b).

(c) A regulated entity shall establish, implement and maintain internal controls and procedures to ensure that its assets are managed in accordance with its overall investment policy, as well as in compliance with applicable accounting requirements and with its legal and regulatory obligations as identified in accordance with paragraph 5.2. These shall ensure that investment procedures are documented and properly overseen. Where appropriate, the functions responsible for measuring, monitoring, settling and controlling asset transactions shall be separate from the regulated entity's front office functions.

(d) The board of a regulated entity shall retain ultimate oversight of, and ensure clear management accountability for, the regulated entity's investment policies and procedures.

(e) The board of a regulated entity shall ensure that any persons involved with a regulated entity's significant investment activities have the appropriate integrity, competence, experience and qualifications for their respective roles in relation to the regulated entity.

(f) A regulated entity shall have rigorous audit procedures that include full coverage of its investment activities to ensure the timely identification and reporting of weaknesses in the regulated entity's internal controls and procedures and any other operating system deficiencies. If the audit is carried out internally it shall be appropriately independent of the function being reviewed.

(g) A regulated entity shall establish, implement and maintain an asset-liability management system (as part of its overall risk management system), including, policies and procedures to ensure on an ongoing basis that its investment activities and asset positions are appropriate to its risk and liability profiles. The regulated entity shall, within its risk management system, take account of the risks associated with mismatches between its assets and liabilities.

(h) A regulated entity shall establish, implement and maintain contingency plans to mitigate the effects of deteriorating investment conditions.

Derivative risk

Derivative risk, in relation to a regulated entity, refers to the risks to which the regulated entity is exposed in relation to its use of derivatives.

Without limiting the investment risk guidance given above, in managing this risk a regulated entity shall apply the following guidance:

(a) The board of a regulated entity that uses, or intends to use, derivatives shall —

(i) collectively have sufficient expertise and understanding of the important issues relating to the use of derivatives so it can properly oversee their use in respect of the regulated entity;

(ii) ensure that any persons conducting and monitoring the derivative activities of the regulated entity have the appropriate integrity, competence, experience and qualifications for their respective roles in relation to the regulated entity;

(iii) establish and maintain appropriate arrangements to verify pricing of its derivatives independently if not quoted on a recognised exchange;

(iv) ensure that the regulated entity has employees with appropriate skills to effectively vet models used by its front office (as applicable) and to price the instruments used, the board shall also ensure that

that pricing follows market convention and that those functions are separate from the regulated entity's front office; and

(v) establish and maintain a risk management system (as part of its overall risk management system) in relation to its use of derivatives, including, but not limited to, internal control framework and sufficient personnel and resources consistent with paragraphs (a)(iv) and (b) to (e).

(b) A regulated entity using, or intending to use, derivatives shall establish implement and maintain an appropriate policy for their use in relation to the regulated entity that shall be approved, monitored and reviewed by its board. This policy shall be consistent with the regulated entity's activities, its overall strategic investment policy, asset-liability management strategy and its risk tolerance limits established by its board. The policy shall address at least the following elements —

(i) the purposes for which derivatives can be used;

(ii) the establishment of appropriately structured exposure limits for derivatives taking into account the purpose of their use and their associated risks;

(iii) restrictions on the holding of certain types of derivatives; and

(iv) appropriate divisions of responsibility and a framework of accountability for derivative transactions.

(c) A regulated entity using, or intending to use, derivatives shall ensure its risk management system encompasses its risks from derivative activities so that the risks arising from all derivative transactions undertaken by the regulated entity can be —

(i) analysed and monitored individually and in aggregate; and

(ii) monitored and managed in an integrated manner with similar risks arising from non-derivative activities so that exposures can be regularly assessed on a consolidated basis.

(d) A regulated entity using, or intending to use, derivatives shall establish implement and maintain internal controls and procedures to ensure that its derivative activities are properly overseen and that transactions have been entered into only in accordance with the regulated entity's policies and procedures, and with its legal and regulatory obligations as identified in accordance with paragraph 5.2. Those controls shall ensure appropriate

segregation between individuals who measure, monitor, settle and control derivatives and individuals who initiate transactions.

(e) Where applicable, the internal audit function of a regulated entity that uses, or intends to use, derivatives, shall establish, implement and maintain rigorous procedures that include coverage of its derivative activities to ensure the timely identification and reporting of weaknesses in the regulated entity's internal controls and procedures, and any other operating system deficiencies. If the audit is carried out internally it shall be appropriately independent of the function being reviewed.

Market risk

Market risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity arising from movements in, or volatility of, market prices and rates. Primarily, this takes the form of changes in the value of the regulated entity's assets and liabilities, both on- and off-balance sheet, whose value may be so affected.

The significance of market risk to the regulated entity is limited to the extent to which an adverse movement in the value of its assets (as a consequence of market movements of financial variables including but not limited to interest rates, foreign exchange rates, equity and other asset prices) is not offset by a corresponding movement in the value of its liabilities, and vice versa.

Market risk encompasses general market risk (on all investments) and specific market risk (on each investment).

Market risk includes the regulated entity's exposure to —

(a) equity and other asset risk – the risk of losses resulting from movements in market values of equities and other assets;

(b) interest rate risk – the risk of losses resulting from movements in interest rates;

(c) currency risk – the risk of losses resulting from movements in exchange rates; and

(d) underlying risk – the risk of losses arising from the exposure of derivatives to movements in the price of the underlying components from which their value is derived; this risk is increased where the derivatives it uses are leveraged, as a small movement in the underlying value can cause a large difference in the value of the derivative in such cases.

Credit risk

Credit risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity resulting from the failure by a person to honour an obligation, whether on- or off-balance sheet, to the regulated entity.

Credit risk includes the regulated entity's exposure to —

(a) default (counterparty) risk – the risk that the regulated entity will not receive the cash flows or assets to which it is entitled, or receipt is delayed or is received only in part, because the party from whom the cash flow or asset is owed defaults on that obligation;

(b) downgrade risk – the risk that changes in the probability of a future default by an obligor will adversely affect the present value of a contract with the obligor today; and

(c) concentration risk – the risk of the regulated entity's increased exposure to losses due to concentration of its credit exposures, including, but not limited to, exposures in a geographical area, economic sector, or with a single counterparty or connected parties.

Liquidity risk

Liquidity risk, in relation to a regulated entity, refers to the possibility that the regulated entity, though it may be solvent, has insufficient liquid assets to meet its obligations as they fall due.

Liquidity risk is often a potential additional factor linked to other risks, including but not limited to —

(a) mismatches between the size and timing of the regulated entity's asset and liability cash flows;

(b) associated investment risk – the risk that an investment by the regulated entity in a member of the regulated entity's group or other associate of the regulated entity might be difficult to sell, or that greater credit risk is accepted by the regulated entity in relation to such counterparties than would ordinarily be the case where a counterparty is not associated with the insurer, or that associates of the regulated entity might create a drain on the financial or operating resources of the regulated entity;

(c) funding risk – the risk that the regulated entity will not be able to obtain sufficient outside financial support when its assets are illiquid and it needs additional liquid assets;

(d) liquidation value risk – the risk that unexpected timings or amounts of cash flows needed by the regulated entity may lead to the liquidation of its assets when market conditions would result in loss of value when realised;

(e) unexpected increase in liability cash flows;

(f) unexpected reduction in asset cash flows;

(g) contractual and other constraints;

(h) policyholder actions;

(i) negative publicity; and

(j) external factors, including, but not limited to, deterioration in the economy, abnormally volatile or stressed markets or political and legal risk.

Operational risk

Operational risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity resulting from disruptions, errors, omissions or other failures in its systems, people or operations.

Group risk

Group risk includes, amongst other things, exposure to the risks inherent in intra-group transactions and arrangements, including, but not limited to, loans and other outstanding balances and guarantees.

Business market and environment risk

Business market and environment risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity resulting from external threats. Adverse business conditions can arise from various sources or combination of sources, including, but not limited to —

(a) political, legislative, economic, sociological and technological factors; and

(b) policyholders, outsourced providers, key business counterparties and competitors.

Business planning risk

Business planning risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity resulting from its use of inappropriate, imprudent or otherwise flawed assumptions when pricing its products, and planning and forecasting in relation to its business activities.

Information technology and communication technology risk

Information technology and communication technology risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity resulting from failure or interruption in operation of its information technology and communication technology systems.

Business continuity and disaster risks

Business continuity and disaster risks, in relation to a regulated entity, refer to the possibility of an adverse impact on the regulated entity resulting from its business being interrupted.

Legal and compliance risk

Legal risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity resulting from the legal action of others, or hindrances in its enforcing a contract with another party.

Compliance risk, in relation to a regulated entity refers to the possibility of an adverse impact on the regulated entity resulting from possible non-compliance with its legal and regulatory obligations.

Crime and fraud risk

Crime and fraud risk, in relation to a regulated entity, refers to the possibility of the regulated entity (including, but not limited to, its directors, senior managers, employees and other persons appointed to act on behalf of the regulated entity) being involved in criminal or civil wrongdoing.

Reputational risk

Reputational risk, in relation to a regulated entity, refers to the possibility of an adverse impact on the regulated entity or its stakeholders due to disrepute caused by the business activities or conduct of the regulated entity or its directors, senior managers, employees or other persons appointed to act on behalf of the regulated entity.

Paragraph 4 and 22.2

SCHEDULE 2

DIRECTORS' CERTIFICATE ON CORPORATE GOVERNANCE

To the Supervisor

_____

(State the name of the regulated entity for which this certificate is given (herein the "regulated entity"))

We certify that:

To the best of our knowledge and belief, throughout the financial period ended (INSERT BALANCE SHEET DATE OF ACCOMPANYING ANNUAL ACCOUNTS), except as specified in the attached report, the regulated entity complied with the requirements of the CGC.

Signed for and on behalf of the board of directors of the regulated entity on (INSERT DATE) by a duly authorised person or persons:

_____

(State name and position held within the regulated entity)

The report referred to above shall include—

1. reference to any instances where the regulated entity has been unable to comply with the requirements of the CGC;
2. the reasons why the regulated entity has been unable to so comply; and
3. actions proposed or taken, including relevant timeframes, to address any matters referred to in paragraph 1.

.....

Made 1 October 2010

Supervisor

Insurance and Pensions Authority