



CORPORATE GOVERNANCE CODE OF PRACTICE FOR INSURERS 2021

Index

Guidance Note	Page
1 Title	5
2 Commencement of these Guidance Notes and withdrawal of previous version	5
3 Introduction	5
4 These Guidance Notes in operation	6
PART 1: GENERAL GOVERNANCE REQUIREMENTS	
5 Application of the CGC	6
6 Additional matters concerning the application of the CGC to permit holders	7
7 Governance requirement and implementation of the CGC	7
8 Directors' Certificate on Corporate Governance	7
9 General conduct	7
10 Compliance	8
11 Financial management	8
12 General management	8
13 Asset protection	9
14 Records	9
15 Governance system documentation	9
16 Business continuity	9
PART 2: BOARD COMPOSITION AND OPERATION	
17 Appointment and removal of directors	9
18 Board composition	10
19 Objective oversight and judgement	10
20 Chairperson and chief executive	10
21 Powers of the board	11
22 Matters reserved to the board	11
23 Frequency of board meetings	11
24 Board meeting documents	11
25 Minutes of board and board committee meetings	12

PART 3: KEY FUNCTIONS AND RESPONSIBILITIES OF THE BOARD		12
26	Ultimate accountability and responsibility, and delegation	12
27	Identification of responsibilities, authority and accountabilities	13
28	Board committees.....	14
29	Directors and senior management.....	14
30	Providers of significant outsourced activities and functions.....	15
31	Standards of conduct	15
32	Business objectives, strategies, significant policies and business plans	15
33	Remuneration policy.....	16
34	Financial reporting system including external audit	16
35	Information and communication systems	17
36	Risk management, financial management and regulatory capital compliance.....	17
37	Internal control system	18
38	Other arrangements	19
39	Culture	19
40	Self assessment.....	19
PART 4: KEY RESPONSIBILITIES OF DIRECTORS		20
41	Directors' responsibilities.....	20
PART 5: KEY RESPONSIBILITIES OF SENIOR MANAGEMENT		20
42	Senior management responsibilities.....	20
PART 6: OUTSOURCED SIGNIFICANT ACTIVITIES AND FUNCTIONS		21
43	Outsourced significant activities and function arrangements	21
PART 7: ACTUARIAL FUNCTION		22
44	Function.....	22
45	Operational requirements	24
46	Objective judgement	25
47	Dual role of appointed actuary and director.....	25
PART 8: INTERNAL AUDIT FUNCTION		25
48	Meaning of “internal audit function” in the CGC	25
49	General.....	26
50	Reporting and recording	27
51	Delegation (including outsourcing).....	27
PART 9: COMPLIANCE FUNCTION		28
52	Meaning of “compliance function” in the CGC.....	28
53	General.....	28
54	Nature and location	29
55	Reporting.....	29

PART 10: EXTERNAL AUDIT	29
56 General	29
57 Engagement letter	29
58 Governance communication	30
PART 11: RISK MANAGEMENT SYSTEM	30
59 General	30
60 System	31
61 Risk management function.....	31
62 Risk identification and measurement	32
63 Risk policy and recording.....	32
64 Risk appetite framework	33
65 Use of risk appetite framework	34
66 Risk responsiveness and feedback loop	34
PART 12: INTERNAL CONTROL SYSTEM	34
67 System	34
68 Internal controls	34
PART 13: OTHER INTERNAL CONTROL ARRANGEMENTS	35
69 Fraud prevention	35
70 Anti-money laundering and combating the financing of terrorism	36
71 Whistleblowing	36
PART 14: FAIR TREATMENT OF POLICYHOLDERS	36
72 Application of requirements (and class 12 requirement).....	36
73 Policyholders	37
74 Member policyholders and participating policyholders	38
PART 15: INTERACTION WITH THE AUTHORITY	39
75 Communication and reporting	39
PART 16: INTERPRETATION	39
76 Meaning of terms	39
SCHEDULE 1 (RISKS)	45
1 General	45
2 Underwriting risk	45
3 Insurance provisions risk.....	46
4 Investment risk.....	47
5 ALM.....	48
6 Derivative risk.....	49
7 Market risk.....	51
8 Credit risk	51
9 Liquidity risk	52

10	Operational risk.....	52
11	Group risk	53
12	Business market and environment risk.....	53
13	Business planning risk.....	53
14	Information technology and communication technology risk	53
15	Business continuity and disaster risks	54
16	Legal and compliance risk	54
17	Crime and fraud risk.....	54
18	Reputational risk	54
19	Strategic risk.....	54
SCHEDULE 2 (ORSA)		55
1	ORSA requirement.....	55
2	General.....	55
3	Responsibility and communication	55
4	Integration	56
5	Policy.....	56
6	Methods, assumptions and coordination of relevant factors.....	56
7	Differences between economic capital needs and regulatory capital requirement.....	58
8	Results, conclusions and additional information	58
9	Records	59
10	Modifications to this schedule for class 12 insurers	60
SCHEDULE 3 (DIRECTORS' CERTIFICATE ON CORPORATE GOVERNANCE)		61
SCHEDULE 4 (SUMMARY ORSA RETURN)		62
ENDNOTES		64
TABLE OF ENDNOTE REFERENCES		64

Statutory Document No. 2021/0276

*Insurance Act 2008*

CORPORATE GOVERNANCE CODE OF PRACTICE FOR INSURERS 2021¹

Laid before Tynwald: 18 January 2022
Coming into Operation: 30 June 2022

The Isle of Man Financial Services Authority issues the following binding Guidance Notes under section 51(1) of the Insurance Act 2008, after carrying out the consultation required by section 51(6) of that Act.

1 Title

These Guidance Notes are the Corporate Governance Code of Practice for Insurers 2021 (in these Guidance Notes, the “CGC”).

2 Commencement of these Guidance Notes and withdrawal of previous version

- (1) These Guidance Notes come into operation on 30 June 2022¹.
- (2) The Corporate Governance Code of Practice for Commercial Insurers (SD 2018/0247) is hereby withdrawn with effect from 30 June 2022.

3 Introduction

Corporate governance, in relation to an insurer, is the system by which the persons who are responsible for the insurer direct, manage 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 insurer’s organisation and business including its constitutional structures and rules, its corporate values, culture and environment, as well as its business and operational objectives, 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 insurer and under which circumstances. It sets out rules for decision

¹ Under section 51(7) of the Insurance Act 2008, Guidance Notes shall be laid before Tynwald as soon as practicable after being issued.

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, an insurer'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 insurer's directors and senior managers, both individually and collectively, and their leadership in promoting a supportive internal culture and environment.

4 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 an insurer's means of having in place 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 insurer. These Guidance Notes should not be used as a substitute for legal advice.

PART 1: GENERAL GOVERNANCE REQUIREMENTS

5 Application of the CGC

- (1) Subject to sub-paragraphs (2) to (5) and paragraph 6, the CGC applies to—
 - (a) authorised insurers; and
 - (b) permit holders,as set out in the CGC.
- (2) Where an insurer has appointed a registered insurance manager to manage its business, the CGC, in respect of the services provided, applies to the insurance manager as an outsourced significant activity or function of the insurer and as part or all of the insurer's executive management (as the case may be).
- (3) In respect of an insurer that is a PCC, the CGC shall apply—
 - (a) separately to the business of its core and each of its cells respectively; or
 - (b) to the PCC as a whole,

as appropriate in the context of the requirement of the CGC in question.

- (4) In sub-paragraph (3), “cell”, “core” and “PCC” have the meanings given in the Insurance Regulations 2021².
- (5) A dormant authorised insurer, in accordance with regulation 18(2) of the Insurance Regulations 2021, is exempt from the CGC.

6 Additional matters concerning the application of the CGC to permit holders

In relation to paragraph 5(1)(b)—

- (a) the CGC does not apply to a permit holder that is authorised to carry on an insurance business in a jurisdiction which has an approved supervisor as defined in regulation 3(1) of the Insurance Regulations 2021; and
- (b) where the CGC does apply to a permit holder—
 - (i) it shall apply only to its activities carried on in or from the Isle of Man;
 - (ii) it shall apply as set out in the CGC (as applicable) and with any other necessary modifications as may be specified in writing by the Authority; and
 - (iii) the Authority may exempt the permit holder in writing from some or all of the requirements of the CGC as stipulated by the Authority.

7 Governance requirement and implementation of the CGC

Pursuant to section 17A of the Act, the board and senior management of an insurer must establish, implement and maintain adequate, appropriate and effective measures that meet the CGC’s requirements in a way that is proportionate to the nature, scale and complexity of the insurer, its activities and the risks to which it is or may be exposed.

8 Directors’ Certificate on Corporate Governance

An insurer must, at the same time as its audited accounts are submitted to the Authority, provide to the Authority a completed certificate in the form set out in Schedule 3.

9 General conduct

- (1) An insurer must carry on its business—
 - (a) with due care, skill and diligence;

² SD 2021/0278

- (b) in a manner that—
 - (i) is honest and straightforward;
 - (ii) ensures its reasonably foreseeable, relevant and material risks are managed adequately, appropriately and effectively;
 - (iii) is consistent with the long-term interests and viability of the insurer; and
 - (iv) adequately recognises and protects the rights, interests and information needs of its policyholders and other stakeholders to ensure that they are treated fairly.
- (2) An insurer's significant systems of governance must, where appropriate, clearly recognise the requirements referred to in sub-paragraph (1) and include the measures necessary to ensure they are achieved in practice.
- (3) An insurer must 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.

10 Compliance

An insurer has an obligation to identify and comply with its legal and regulatory obligations and must take all reasonable steps to do so.

11 Financial management

An insurer must—

- (a) maintain adequate capital and other financial resources to meet its economic capital needs;
- (b) maintain sufficient asset liquidity to meet its liabilities as they fall due; and
- (c) evaluate at appropriate intervals in advance its—
 - (i) risks and options; and
 - (ii) where appropriate, intentions,under possible scenarios where the insurer would need to recover from severely adverse circumstances (including its hypothetical insolvency).

12 General management

An insurer must have an appropriate level of management, with adequate and appropriate resources, including human resources (whether employed or outsourced) with appropriate competence and integrity for their individual and

collective roles in relation to the insurer, that provides for its sound and prudent management.

13 Asset protection

An insurer must take all reasonable steps to safeguard its assets and any other assets in its keeping.

14 Records

An insurer must—

- (a) keep proper books, accounts and documents, including documentation of its internal organisation, (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 orderly and readily accessible in or from the Isle of Man and available for inspection and investigation by or on behalf of the Authority; and
- (c) without limiting any other applicable retention requirement or other legal requirement upon the insurer to dispose of, rectify or protect personal data in accordance with data protection legislation, keep such records for at least six years from the date on which the record is made or, if later, it ceases to be relevant.

15 Governance system documentation

An insurer must establish and maintain adequate and appropriate documentation in respect of its significant systems of governance (for example, its risk management system including internal controls system) and their operation.

16 Business continuity

An insurer must 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, appropriate and effective arrangements to ensure that it can continue to function effectively and comply with its legal and regulatory obligations (as identified in accordance with paragraph 10) in the event of an anticipated or unforeseen disruption.

PART 2: BOARD COMPOSITION AND OPERATION

17 Appointment and removal of directors

An insurer must establish, implement and maintain a documented and transparent board nomination, election and removal process.

18 Board composition

- (1) The board of an insurer must include an adequate and appropriate number and mix of directors, with an overall adequate and appropriate combined level of knowledge, skills, experience and commitment for such roles, which is commensurate with the insurer's risk profile, including its governance framework, such that it can properly discharge its duties and responsibilities and carry out its functions in relation to the insurer.
- (2) Subject to sub-paragraphs (3) to (6), the board of an insurer must include at least—
 - (a) one independent non-executive director; and
 - (b) two directors who are resident in the Isle of Man.
- (3) The requirement under sub-paragraph (2)(b) is reduced such that the board of an insurer that—
 - (a) is dormant; or
 - (b) has appointed a registered insurance manager to manage its day-to-day operations,must include at least one director who is resident in the Isle of Man.
- (4) An insurer is exempt from sub-paragraph (2)(a) if it—
 - (a) is dormant; or
 - (b) has obtained the Authority's prior written approval to be so exempt.
- (5) A permit holder is exempt from sub-paragraph (2)(b).
- (6) Where the relevant requirements are met in each case, a director referred to in sub-paragraph (2)(a) may be the same individual as a director referred to in sub-paragraph (2)(b) or (3).

19 Objective oversight and judgement

The board of an insurer must—

- (a) be able to exercise objective and independent oversight, judgement and decision making in relation to the insurer; and
- (b) establish, implement and maintain adequate, appropriate and effective internal governance practices and procedures to support the board in this regard.

20 Chairperson and chief executive

An insurer must not combine the roles of chairperson and chief executive (or equivalent) in one individual in respect of the insurer.

21 Powers of the board

The board of an insurer must 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 insurer. For this purpose the board must, amongst other things, be able to—

- (a) obtain timely, accurate, relevant and sufficiently comprehensive information and analyses relating to the insurer, its management and external environment;
- (b) delegate activities and functions as appropriate; and
- (c) obtain external expertise where necessary and as appropriate.

22 Matters reserved to the board

The board of an insurer must—

- (a) establish, implement 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 insurer which is adequate, appropriate and effective such that the board can properly discharge its duties and responsibilities and carry out its functions in relation to the insurer; 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, appropriate and effective.

23 Frequency of board meetings

The board of an insurer must meet with sufficient regularity so that it can properly discharge its duties and responsibilities and carry out its functions in relation to the insurer.

24 Board meeting documents

- (1) The board of an insurer must, where reasonably practicable and appropriate, ensure in respect of each meeting of the board that the following are circulated to its directors in advance of the meeting to allow directors adequate time to consider their content—
 - (a) a suitably detailed agenda of the items to be considered at the meeting;
 - (b) the minutes from the previous meeting of the board; and
 - (c) adequate and appropriate information in support of the matters to be considered at the meeting.
- (2) Sub-paragraph (1) does not inhibit appropriate flexibility for the board of an insurer to carry out its duties and responsibilities, including in respect

of meetings of the board, such as having limited agenda and short notice meetings, deferring matters to a subsequent meeting and raising other business at a meeting.

25 Minutes of board and board committee meetings

- (1) The board of an insurer must ensure that the insurer keeps minutes and associated documents of all of its board and board committee meetings. These must provide an adequate and appropriate record of corresponding proceedings including –
 - (a) which directors attended, which alternate directors attended as an alternate (and for whom) and which directors did not attend for any reason;
 - (b) sufficient detail to evidence what board-level attention was given at the meeting to matters being considered at the meeting and the substance of discussions had at the meeting;
 - (c) all material considerations, decisions and actions (including actions taken and points for further action, as applicable);
 - (d) any conflicts of interest arising in relation to the matters being considered at the meeting and how they were managed; and
 - (e) any dissensions or negative votes recorded in terms acceptable to the dissenting person or negative voter (for the avoidance of doubt, this is without prejudice to any situation where a director feels he or she should resign).
- (2) The minutes referred to in sub-paragraph (1) must –
 - (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.

PART 3: KEY FUNCTIONS AND RESPONSIBILITIES OF THE BOARD

26 Ultimate accountability and responsibility, and delegation

- (1) The board of an insurer is ultimately accountable and responsible for the affairs of the insurer. Delegating authority to board committees, management or others does not absolve the board of its duties and responsibilities in relation to the insurer.
- (2) Where the board of an insurer delegates any of its activities or functions in relation to the insurer, it must only do so in a manner that does not –

- (a) dilute its ultimate accountability in relation to the insurer;
 - (b) reduce its ability to discharge properly its duties and responsibilities or carry out its activities and functions in relation to the insurer; or
 - (c) lead to any person having unfettered powers in relation to the insurer.
- (3) The board of an insurer must ensure that any authority it has delegated to carry out any activity or function in relation to the insurer is properly authorised, communicated and documented.
- (4) Notwithstanding any delegation, the board of an insurer must provide sound and prudent oversight in relation to the insurer's affairs, and accordingly it must—
- (a) ensure it receives timely, accurate, relevant and sufficiently comprehensive information and analyses relating to the insurer, its management and external environment such that it can properly discharge its duties and responsibilities and carry out its functions in relation to the insurer;
 - (b) ensure that the insurer has taken all reasonable steps to identify and comply with its legal and regulatory obligations in accordance with paragraph 10;
 - (c) satisfy itself that the strategies, significant policies and procedures it has established in relation to the insurer have been properly implemented and are being adhered to;
 - (d) satisfy itself that the corporate culture it has established in relation to the insurer has been properly embedded; and
 - (e) satisfy itself that any activities or functions it has delegated in relation to the insurer have been responsibly and prudently carried out, and any authority it has delegated has not been exceeded.

27 Identification of responsibilities, authority and accountabilities

The board of an insurer must—

- (a) establish, implement and maintain, clear definitions of, and distinguish between, the roles, responsibilities, decision-making, interaction and cooperation of—
 - (i) the insurer's board;
 - (ii) any board committees of the insurer;
 - (iii) any chairperson and chief executive (or equivalent) of the insurer;
 - (iv) the insurer's senior management; and
 - (v) any outsourced provider of a significant activity or function of the insurer,

- including to promote and sustain an appropriate separation of its oversight function (including, where appropriate, independent control functions) and management responsibilities;
- (b) establish, implement and maintain decision-making processes and divisions of responsibility that ensure an appropriate balance of power and authority for the insurer, so that—
 - (i) no person has unfettered powers of decision in relation to the insurer; and
 - (ii) contractual arrangements and other transactions of the insurer are only entered into with appropriate authority; and
 - (c) satisfy itself that the insurer is organised and controlled in a way that provides for its sound and prudent management, including ensuring accountability to the board and proper oversight by the board of any committees of the board, the insurer's senior management and any outsourced provider of a significant activity or function of the insurer.

28 Board committees

- (1) The board of an insurer must assess the need for and, where appropriate, establish committees of the board.
- (2) Where such a committee is established, the board must—
 - (a) define adequate and appropriate terms of reference of the committee and these must 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 insurer; and
 - (c) ensure that the committee's terms of reference are in writing and are made available to relevant parties, including the insurer's senior management (where appropriate) and external auditor.

29 Directors and senior management

The board of an insurer must—

- (a) establish, implement and maintain the means by which the insurer's senior management is monitored and held accountable to the board;
- (b) subject to sub-paragraph (c) insofar as its powers permit—

- (i) approve the selection, appointment, removal and any applicable succession planning of the insurer's directors and senior management; and
 - (ii) ensure that the insurer's individual directors and senior managers possess the appropriate integrity, competence, experience and qualifications for their respective roles in relation to the insurer; and
- (c) where the insurer's senior management is outsourced to a registered insurance manager, paragraph 30 shall apply instead of sub-paragraph (b).

30 Providers of significant outsourced activities and functions

The board of an insurer must—

- (a) ensure that the arrangements for any outsourced significant activity or function of the insurer are consistent with Part 6; and
- (b) approve the selection, appointment, removal and any applicable succession planning of any outsourced provider of a significant activity or function of the insurer.

31 Standards of conduct

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

- (a) conflicts of duty or interest in relation to the insurer;
- (b) matters in relation to the insurer 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 insurer's stakeholders.

32 Business objectives, strategies, significant policies and business plans

The board of an insurer must—

- (a) establish, implement and maintain in relation to the insurer adequate and appropriate—
 - (i) business objectives; and
 - (ii) strategies and significant policies for achieving those objectives for all of its significant business decision areas;

- (b) establish and maintain the means for implementing those objectives, strategies and policies;
- (c) review and approve the significant business plans of the insurer;
- (d) evaluate at appropriate intervals, and at least annually, the insurer's performance against those business plans in light of those strategies and policies; and
- (e) review the objectives, strategies and significant policies of the insurer at appropriate intervals, and at least annually, and adapt them as necessary to ensure they remain adequate, appropriate and effective in relation to the insurer in light of any relevant and material changes in the insurer's internal or external environment.

33 Remuneration policy

The board of an insurer must—

- (a) establish, implement and maintain an adequate, appropriate and effective remuneration policy for persons whose actions may have a material impact on the insurer, including its directors, senior managers (including notably its principal control officers), employees and any outsourced provider of a significant activity or function of the insurer (as applicable);
- (b) ensure that the remuneration policy—
 - (i) does not induce inappropriate behaviour, including excessive or inappropriate risk-taking in relation to the insurer;
 - (ii) is in line with the insurer's corporate culture, objectives, strategies and significant policies (including its risk appetite framework), and long term interests and viability;
 - (iii) has proper regard to the interests of the insurer's policyholders and other stakeholders; and
 - (iv) mitigates any relevant conflicts of interest; and
- (c) ensure that in respect of the establishment, implementation and maintenance (including reviews) of the remuneration policy that any relevant conflicts of interest are identified and properly managed and documented.

34 Financial reporting system including external audit

The board of an insurer must—

- (a) establish, implement and maintain a system (including processes) for the insurer's financial reporting that ensures the integrity,

reliability and transparency of that reporting both for public, where applicable, and regulatory purposes;

- (b) ensure that this is supported by clearly defined roles and responsibilities of the board, the insurer's senior management and external auditor; and
- (c) ensure that there is adequate, appropriate and effective direction and oversight of the insurer's external audit process.

35 Information and communication systems

The board of an insurer must establish, implement and maintain information and other communication systems in relation to the insurer which—

- (a) are reliable;
- (b) ensure the prompt and effective transfer of information between—
 - (i) all levels of management within the insurer;
 - (ii) the insurer and any outsourced provider of a significant activity or function of the insurer; and
 - (iii) the insurer and its stakeholders; and
- (c) are secure such that the insurer's information is safeguarded.

36 Risk management, financial management and regulatory capital compliance

The board of an insurer must—

- (a) establish, implement and maintain a risk management system for the insurer that is consistent with Part 11 (including Schedules 1 and 2);
- (b) allocate responsibility for, and ensure it receives—
 - (i) risk management information and assessments in accordance with paragraph 66(b); and
 - (ii) ORSA reports as referred to in paragraph 9(c) and, where applicable, 10(1)(c)(i) of Schedule 2;
- (c) establish, implement and maintain the risk strategies and significant risk policies and procedures of the insurer, including its risk appetite framework;
- (d) review at appropriate intervals, and at least annually, the insurer's—
 - (i) relevant and material risks;
 - (ii) risk profile;

- (iii) risk strategies and significant risk policies and procedures, including its risk appetite framework, capital adequacy policy, liquidity adequacy policy, and the insurer's compliance with same; and
- (iv) risks, options and, where appropriate, intentions in possible recovery scenarios;
- (e) assess at appropriate intervals, and at least annually, the insurer's current and prospective economic capital needs, capital adequacy, liquidity adequacy and regulatory capital compliance; and
- (f) take any action necessary to ensure that the insurer –
 - (i) adequately, appropriately and effectively manages all of its relevant and material risks;
 - (ii) complies with its capital adequacy requirement, liquidity adequacy requirement and regulatory capital requirement;
 - (iii) properly assesses its ability over its forecast time horizon to continue to comply with its capital adequacy requirement, liquidity adequacy requirement and regulatory capital requirement; and
 - (iv) has a properly considered approach in respect of possible recovery scenarios.

37 Internal control system

The board of an insurer must, as part of the insurer's risk management system –

- (a) establish, implement and maintain an internal control system for the insurer that is consistent with Part 12;
- (b) allocate responsibility for, and ensure it receives, reports in accordance with paragraphs 50 and 55, and as appropriate from the insurer's actuarial function (including reports in accordance with paragraph 44(4)(e));
- (c) ensure timely action is taken, where necessary, to correct any identified –
 - (i) weaknesses or deficiencies in the insurer's internal controls, procedures or other systems of governance;
 - (ii) material instances of non-compliance with the insurer's internal policies or procedures; and
 - (iii) non-compliance with the insurer's legal or regulatory obligations; and
- (d) review at appropriate intervals, and at least annually, the insurer's material –
 - (i) internal controls;

- (ii) procedures; and
- (iii) other systems of governance,

in a manner that is consistent with Part 8, 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).

38 Other arrangements

The board of an insurer must ensure that the insurer has in place arrangements for—

- (a) fraud prevention in accordance with paragraph 69;
- (b) anti-money laundering and combatting the financing of terrorism in accordance with paragraph 70;
- (c) whistleblowing in accordance with paragraph 71;
- (d) fair treatment of policyholders in accordance with Part 14 (as applicable) and the other requirements in the CGC relevant to the fair treatment of policyholders and other stakeholders; and
- (e) interaction with the Authority in accordance with Part 15.

39 Culture

The board of an insurer must promote and sustain a corporate culture in respect of, and throughout, the insurer that supports the—

- (a) implementation of a corporate governance framework that meets, on an ongoing basis, the requirements of the CGC that are applicable to the insurer; and
- (b) implementation of the insurer's objectives, strategies and significant policies.

40 Self assessment

The board of an insurer must at appropriate intervals, and at least annually, evaluate its own composition (as referred to in paragraphs 18(1) and 19(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 insurer.

PART 4: KEY RESPONSIBILITIES OF DIRECTORS

41 Directors' responsibilities

A director of an insurer must—

- (a) act on a well-informed basis;
- (b) act in good faith, honestly and reasonably;
- (c) exercise due care, skill and diligence;
- (d) act in the best interests of the insurer and its policyholders, putting those interests ahead of his or her own interests;
- (e) exercise independent judgement and objectivity in his or her decision making, taking due account of the interests of the insurer and its policyholders;
- (f) identify and either avoid or promptly disclose to the board of the insurer any conflicts of duty or interest he or she has or may have in relation to the insurer;
- (g) not use his or her position to gain undue personal advantage or cause any detriment to the insurer;
- (h) ensure he or she has the appropriate integrity, competence, experience, qualifications and commitment so he or she can properly discharge his or her duties and responsibilities and carry out his or her functions in relation to the insurer; and
- (i) properly discharge his or her duties and responsibilities and carry out his or her functions in relation to the insurer.

PART 5: KEY RESPONSIBILITIES OF SENIOR MANAGEMENT

42 Senior management responsibilities

The senior management of an insurer must—

- (a) manage the day-to-day operations of the insurer soundly and prudently, ensuring those operations are carried out effectively and in accordance with the insurer's—
 - (i) objectives, strategies, policies (including its risk appetite framework) and procedures established by its board;
 - (ii) general conduct requirements under paragraph 9;
 - (iii) legal and regulatory obligations as identified in accordance with paragraph 10;

- (b) establish, implement and maintain adequate, appropriate and effective internal controls and procedures in respect of the insurer to ensure compliance with sub-paragraph (a);
- (c) promote and sustain in respect of, and throughout, the insurer a corporate culture consistent with the requirements of paragraph 39;
- (d) individually identify and either avoid or promptly disclose to the board of the insurer any conflicts of duty or interest he or she has or may have in relation to the insurer;
- (e) provide the insurer's board with timely, accurate, relevant, and sufficiently comprehensive reports, analysis or other information (in a manner consistent with the role and responsibilities of senior management) to enable the board to carry out its duties and functions, including the monitoring and review of—
 - (i) the insurer's performance and the performance of its senior management;
 - (ii) the insurer's reasonably foreseeable, relevant and material risks, risk profile, capital adequacy, liquidity adequacy and regulatory capital compliance positions;
 - (iii) the insurer's business strategy, policies and business plans established by the board in relation to the insurer; and
 - (iv) such other matters in relation to the insurer as the board may specify;
- (f) provide the insurer'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; and
- (g) ensure that the insurer maintains records in accordance with paragraphs 14 and 15.

PART 6: OUTSOURCED SIGNIFICANT ACTIVITIES AND FUNCTIONS

43 Outsourced significant activities and function arrangements

Where a significant activity or function of an insurer has been outsourced, the insurer must ensure that—

- (a) it retains at least the same degree of oversight of, and accountability for, the outsourced activity or function as would apply if the outsourced activity or function was not outsourced;
- (b) where the outsourced provider is required to have any regulatory consents in order to carry out the outsourced activity or function, those consents have been obtained and remain in force;

- (c) the outsourced provider has the appropriate integrity, competence, experience and qualifications to carry out the outsourced activity or function;
- (d) the outsourced provider has the capacity to carry out the outsourced activity or function taking into account the size and timing of corresponding workloads;
- (e) its use of the outsourced provider is consistent with the—
 - (i) ongoing and effective risk management, financial management and compliance of the insurer, including not unreasonably increasing its operational risk;
 - (ii) standard of control that would apply if the outsourced activity or function was carried out internally by the insurer;
 - (iii) fair treatment of the insurer's stakeholders (as applicable);
 - (iv) effective operation of the external audit of the insurer; and
 - (v) ongoing, open, honest and timely communication with the Authority in relation to the activities of the insurer, and not unreasonably impairing the Authority's ability to monitor the insurer's compliance with its legal and regulatory obligations; and
- (f) a written agreement is in place with the outsourced provider, where the board of the insurer 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 insurer in relation to the outsourced activity or function.

PART 7: ACTUARIAL FUNCTION

44 Function

- (1) Part 7 applies—
 - (a) to a class 1, 2 or 10 insurer or any combination thereof; and
 - (b) subject to sub-paragraphs (5) and (6), to a class 3 to 9 or 11 insurer or any combination thereof.
- (2) Subject to sub-paragraph (7), a class 12 insurer is exempt from Part 7.

- (3) An insurer must have an effective actuarial function that is adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is or may be exposed.
- (4) An insurer's actuarial function must—
 - (a) have the necessary authority, independence and resources to carry out its activities effectively;
 - (b) be capable of evaluating and providing adequate and appropriate advice to the insurer's board and senior management (and any other relevant person in relation to the insurer) regarding actuarial matters, including those relating to the insurer's technical provisions, premium and pricing activities, capital adequacy and liquidity adequacy, reinsurance, and compliance with its legal and regulatory obligations which are relevant to the actuary's role in respect of the insurer;
 - (c) carry out appropriate activities, including—
 - (i) coordinate the calculation of the insurer's technical provisions;
 - (ii) ensure the appropriateness of the methodologies and underlying models used by the insurer as well as the assumptions made in the calculation of its technical provisions;
 - (iii) assess the sufficiency and quality of the data used in the calculation of the insurer's technical provisions;
 - (iv) compare the best estimates contained within the insurer's technical provisions against relevant experience;
 - (v) inform the insurer's board or its senior management (as appropriate) of the reliability and adequacy of the calculation of the insurer's technical provisions;
 - (vi) oversee the calculation of the insurer's technical provisions and, in particular, in cases where approximations are used in the calculation of best estimates contained within the technical provisions (which may be the case where there is insufficient data of appropriate quality to apply a reliable actuarial method);
 - (vii) express an opinion on the insurer's overall underwriting policy;
 - (viii) express an opinion on the adequacy of the insurer's reinsurance (and any other risk transfer mechanism) arrangements; and
 - (ix) contribute to the effective implementation of the insurer's risk management system and in particular with respect to the risk assessment underlying the determination of its

economic capital needs and corresponding assessment of its capital adequacy and liquidity adequacy and regulatory capital compliance;

- (d) be carried out by persons who have knowledge of actuarial and financial mathematics commensurate with the nature, scale and complexity of the risks inherent in the business and prospective business of the insurer and who are able to demonstrate their relevant experience and applicable professional standards; and
 - (e) provide a report to the board of the insurer at appropriate intervals and at least annually, and that report must at a minimum—
 - (i) document all tasks (and, in particular, those tasks required of the actuarial function in accordance with this Part) that have been undertaken by the actuarial function;
 - (ii) include the results of those activities;
 - (iii) clearly identify any deficiencies; and
 - (iv) give recommendations to the board as to how such deficiencies should be remedied.
- (5) Subject to sub-paragraph (6), in relation to an insurer carrying on business within classes 3 to 9 or 11 (or any combination thereof), the Authority may modify (including reduce) in writing some or all of the requirements of Part 7 where the Authority considers it appropriate to do so.
- (6) Where considering a reduction in requirement as referred to in sub-paragraph (5) in relation to an insurer, the Authority may require the insurer to show to the Authority's satisfaction why the actuarial requirements in question warrant such reduction.
- (7) A class 12 insurer must have, or have access to, an effective actuarial function capable of evaluating and providing advice to the insurer regarding, at a minimum, technical provisions, premium and pricing activities, and compliance with related statutory and regulatory requirements.

45 Operational requirements

An insurer must—

- (a) insofar as it is necessary for the performance of its actuarial function's activities in relation to the insurer, afford the actuarial function the right of direct access at all reasonable times to—
 - (i) the board,
 - (ii) the directors, senior management and other employees and functions;
 - (iii) any outsourced provider of a significant activity or function;

- (iv) the external auditor; and
 - (v) all information and data, of the insurer; and
- (b) require the actuarial function, in relation to its activities, to report to the board of the insurer on a timely basis on relevant actuarial matters, including in accordance with paragraph 44(4)(e).

46 Objective judgement

An actuarial function of an insurer, in forming and formulating its actuarial opinions and advice in respect of the insurer, must be objective and free from any undue influence (for example, from other functions, directors, management or other employees of the insurer) and provide its opinions and advice to the board and Authority (as applicable) in an independent manner.

47 Dual role of appointed actuary and director

- (1) The positions of appointed actuary and director must not ordinarily 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.
- (2) Where the posts of appointed actuary and director are combined, the insurer's board must—
- (a) establish, implement and maintain adequate, appropriate and effective internal controls to ensure that the appointed actuary remains objective and free from any undue influence such that his or her opinions and advice to the board and Authority (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 appointed actuary and director to ensure they remain valid; and
 - (ii) the internal controls established under sub-paragraph (a) to ensure they remain adequate, appropriate and effective.

PART 8: INTERNAL AUDIT FUNCTION

48 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 or may be 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 10.

49 General

- (1) An insurer must 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 or may be exposed, and accordingly, an insurer must ensure that its internal audit function—
 - (a) has appropriate independence from the operational activities it audits;
 - (b) is capable of providing the insurer's board with adequate, appropriate and independent assurance in respect of the quality and effectiveness of the insurer's corporate governance framework;
 - (c) has direct reporting lines to the insurer's board (or audit committee);
 - (d) has sufficient authority and status within the insurer to ensure that the directors and senior management of the insurer react appropriately to its enquiries and recommendations;
 - (e) 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 activity or 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;
 - (f) 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;
 - (g) employs a methodology that identifies the material risks to which the insurer is or may be exposed and allocates its resources accordingly; and

- (h) encompasses both internal and any outsourced functions of the insurer.
- (2) Pursuant to sub-paragraph (1)(g), in relation to an insurer and to avoid any doubt, the CGC allows for an internal audit process to be applied on a proportionate basis over time. This includes keeping under review a work plan for internal audit that is adequate, appropriate and effective for the insurer, its activities and the risks to which it is or may be exposed. An internal audit work plan may schedule work over periods of more than one year provided that the relevant and material systems of governance are addressed at appropriate times. It is not a mandatory requirement for internal audit to be carried out at least every year in respect of every system of governance. Instead it is the responsibility of the insurer's board, together with its internal audit function, to determine an appropriate schedule and focus for internal audit work (including any ad-hoc work the board may require). It is the board's responsibility to ensure that internal audit provides it with such independent assurances as the board needs from internal audit, and at appropriate times given the insurer's circumstances, in order to properly discharge its duties and responsibilities and carry out its functions in relation to the insurer.

50 Reporting and recording

- (1) The findings and recommendations of an insurer's internal audit function must be reported in writing at appropriate intervals, and at least annually in respect of non-class 12 insurers, to the insurer's board.
- (2) Those reports must 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 sub-paragraphs (a) to (d), the reports must either make remedial recommendations as may be necessary or must include a statement in each case that no such matters have been identified.

51 Delegation (including outsourcing)

The insurer's internal audit function may be carried out by one or more suitable resources, including—

- (a) from within the insurer (but a suitable resource does not include a director of the insurer);

- (b) where the insurer is part of a group, its group's internal audit function or other resource from within its group;
- (c) where the insurer has an appointed insurance manager —
 - (i) the internal audit function of the insurance manager or other resource from within the insurance manager; or,
 - (ii) where the insurance manager is part of a group, that group's internal audit function or other resource from within that group; or
- (d) an external party,

and, to avoid any doubt, to be suitable, such a resource must meet the relevant requirements of this Part.

PART 9: COMPLIANCE FUNCTION

52 Meaning of “compliance function” in the CGC

The compliance function of an insurer is the means applied by the insurer to—

- (a) identify and understand the insurer's legal and regulatory obligations in accordance with paragraph 10; and
- (b) establish, implement and maintain compliance strategies, policies, procedures and training,

in order to ensure that the insurer complies with its legal and regulatory obligations as identified in accordance with in paragraph 10.

53 General

An insurer must have an ongoing and effective compliance function that is adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is or may be exposed, and includes the compliance function—

- (a) having adequate and appropriate expertise, resources, authority and independence to carry out its activities effectively; and
- (b) being capable of adequately and appropriately assisting the insurer to—
 - (i) identify and meet its legal and regulatory obligations; and
 - (ii) promote and sustain a sound compliance culture in respect of the insurer, including through the monitoring of related internal policies.

54 Nature and location

- (1) Without limiting paragraph 52 or 53, the compliance function of an insurer—
 - (a) may be carried out internally by the insurer or by a suitable external party or a combination of both;
 - (b) must be ultimately controlled in or from the Isle of Man (a permit holder is exempt from this sub-paragraph); and
 - (c) must be substantially carried out in or from the Isle of Man or, where operational functions of the insurer are carried out outside of the Isle of Man, the insurer'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.
- (2) For the avoidance of doubt, this paragraph does not restrict an insurer from obtaining advice from outside of the Isle of Man as appropriate to its activities.

55 Reporting

The compliance function of an insurer must report at appropriate intervals, and at least annually, to the insurer's board on compliance matters in accordance with its role in relation to the insurer.

PART 10: EXTERNAL AUDIT**56 General**

An insurer must—

- (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 Authority such information and confirmations as the Authority requests for the purposes of carrying out of the functions of the Authority.

57 Engagement letter

Prior to commencement of its audit, an insurer must obtain from its external auditor a letter of engagement which—

- (a) contains an undertaking of the external auditor to provide to the insurer, and upon request provide to the Authority a copy of, the governance communications referred to in paragraph 58;

- (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.

58 Governance communication

- (1) An insurer must at the same time as its audited accounts are submitted to the Authority—
 - (a) provide to the Authority a copy of the communication, in relation to those accounts, made by its external auditor to those charged with the insurer’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 Authority whether the insurer 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 insurer receives no ISA 260 or ISA (UK and Ireland) 260 communication, or equivalent, provide the Authority with a copy of its external auditor’s confirmation that no such communication has been or is anticipated to be issued.
- (2) An insurer must, without undue delay, provide to the Authority a copy of any other formal communication it receives from its external auditor that identifies any material weakness relating to the insurer’s internal controls, procedures or other systems of governance.

PART 11: RISK MANAGEMENT SYSTEM

59 General

An insurer must—

- (a) establish, implement and maintain (and operate within) an effective risk management system, including risk management function, that is adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is or may be exposed, and is consistent with paragraphs 60 to 66;
- (b) establish and 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;
- (c) integrate its risk management system into its decision making processes so that decisions can be taken with due regard for the risks involved; and

- (d) base its risk management actions on due consideration of its economic capital needs, its regulatory capital requirement and the nature and amount of its financial resources, including making appropriate use of its ORSA.

60 System

The risk management system of an insurer must—

- (a) be ongoing and comprehensive including 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, relevant and material risks to which the insurer is or may be exposed;
- (b) encompass all such risks on an individual and aggregate basis, including the risks referred to in Schedule 1 (as applicable);
- (c) establish, implement and maintain adequate, appropriate and effective risk categories and risk management policies for all of its relevant and material risks, including in respect of ALM, investment activities and underwriting;
- (d) ensure that the operations and risk exposures of the insurer are within the risk appetite framework established by its board in respect of the insurer in accordance with paragraphs 64 and 65; and
- (e) include an ERM framework which—
 - (i) includes an ORSA process in accordance with Schedule 2, which coordinates and integrates the insurer's risk and financial management in respect of the insurer as a whole, including, notably, for the purposes of ensuring it complies on an ongoing basis with its capital adequacy requirement, liquidity adequacy requirement and regulatory capital requirement; and
 - (ii) reflects the relationship between the insurer's risk profile, risk appetite framework, economic capital needs, capital adequacy, liquidity adequacy and regulatory capital requirement, and its processes and methods for monitoring its risks.

61 Risk management function

- (a) An insurer must have an ongoing and effective risk management function to manage its risk management system.
- (b) An insurer's risk management function must have the necessary authority, independence and resources to carry out its activities

effectively, and be capable of assisting the insurer, in a manner consistent with this Part, to—

- (i) identify, assess, measure, monitor, control and mitigate its risks;
- (ii) report on its relevant and material risks; and
- (iii) promote and sustain a sound risk culture in respect of the insurer.

62 Risk identification and measurement

- (1) An insurer's ERM framework must provide for the identification of its reasonably foreseeable, relevant and material risks and their interdependencies, as well as their quantification under a sufficiently wide range of adverse outcomes, including by using processes and techniques which are adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is or may be exposed for the purposes of—
 - (a) supporting its risk management activities;
 - (b) determining its economic capital needs;
 - (c) assessing its current and prospective capital adequacy;
 - (d) assessing its current and prospective liquidity adequacy; and
 - (e) assessing its prospective compliance with its regulatory capital requirement.
- (2) In sub-paragraph (1), "techniques" include forward-looking quantitative methods, including such stress testing, reverse stress testing and scenario analysis as may be adequate and appropriate for the purpose in question.
- (3) Pursuant to sub-paragraphs (1) and (2) an insurer's ERM framework must also encompass identifying and assessing the insurer's prospective risks over its forecast time horizon.

63 Risk policy and recording

- (1) An insurer's ERM framework must include a risk management policy which—
 - (a) outlines how all of the insurer's relevant and material categories of risk are managed within the insurer's risk appetite as established by its board in respect of the insurer in accordance with paragraph 64 and, where appropriate, coordinated in respect of both its business strategy and its day to day operations;
 - (b) considers a period of at least the insurer's forecast time horizon; and
 - (c) describes the relationship between the insurer's risk profile, risk appetite framework, economic capital needs, capital adequacy,

liquidity adequacy and regulatory capital requirement, and its processes and methods for monitoring its risks.

- (2) An insurer's ERM framework must support the measurement of its risks by providing accurate documentation with appropriately detailed descriptions and explanations of those risks, the measurement approaches used and the key assumptions made.

64 Risk appetite framework

- (1) An insurer's ERM framework must include a risk appetite framework setting out—
 - (a) a risk appetite statement which articulates the aggregate level and types of risk the insurer is willing to assume within its risk capacity to achieve its financial and strategic objectives and business plans (taking into account all of the insurer's reasonably foreseeable, relevant and material risks and their interdependencies within the insurer's current and prospective risk profiles);
 - (b) in respect of each of its relevant and material categories of risk, pursuant to and within its risk appetite—
 - (i) risk limits, which are policy statements specifying qualitatively and, where reasonably practicable, quantitatively the category of risk and, subject to sub-paragraph (ii), the aggregate amount of that risk the insurer is willing to assume; and
 - (ii) a risk tolerance, in relation to each risk limit, which is the acceptable variability around (including above) that limit.
- (2) An insurer's risk capacity, as referred to in sub-paragraph (1)(a), is the maximum amount of risk the insurer is able to assume before breaching one or more of its significant constraints, including its capital adequacy requirement, liquidity adequacy requirement and regulatory capital requirement.
- (3) The risk limits and tolerances, as referred to in sub-paragraph (1)(b), must take account of any relevant relationship between the categories of risk which might materially impact upon those risks.
- (4) If an insurer is or may be exposed to a risk which is plausibly relevant and material but is not practicably quantifiable (and therefore not readily able to be aggregated for risk appetite purposes), the insurer must by way of its ORSA—
 - (a) make a qualitative assessment which is appropriate to the risk and sufficiently detailed to be useful for its risk management and financial management purposes; and
 - (b) identify and explain how the exposure is otherwise addressed by the insurer's risk management and financial management policies.

65 Use of risk appetite framework

An insurer must—

- (a) make appropriate use of its risk limits and risk tolerances in its business strategies and plans, including ensuring that it does not exceed its risk appetite; and
- (b) integrate and use its risk limits and risk tolerances in its day-to-day operations, including in a manner which prevents the insurer from exceeding its risk appetite and promptly brings any breaches of its risk limits or risk tolerances to the attention of its management.

66 Risk responsiveness and feedback loop

An insurer's ERM framework must—

- (a) be responsive to changes in its risk profile, whether arising from internal or external events; and
- (b) incorporate a feedback loop, based on timely, appropriate and good quality information, management processes and objective assessment, which enables the insurer to take any necessary risk management actions in a timely manner in response to changes in its internal or external risk environment.

PART 12: INTERNAL CONTROL SYSTEM

67 System

- (1) The internal control system of an insurer is part of its risk management system and includes its—
 - (a) actuarial function as referred to in Part 7;
 - (b) internal audit function as referred to in Part 8;
 - (c) compliance function as referred to in Part 9; and
 - (d) internal controls as referred to in paragraphs 68 to 71.
- (2) An insurer's risk management system must have due regard for any relevant and material findings and recommendations communicated to the insurer by its component functions (as referred to in sub-paragraph (1)), and its external auditor.

68 Internal controls

- (1) An insurer must establish, implement and maintain (and operate within) effective internal controls including—
 - (a) arrangements for delegating authority and segregation of duties; and
 - (b) other checks and balances.

- (2) These must be adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is or may be exposed to ensure that the insurer and other persons (as applicable) adhere to the—
 - (a) insurer's strategies, policies and procedures established by its board;
 - (b) requirements of the CGC; and
 - (c) insurer's other legal and regulatory obligations as identified in accordance with paragraph 10.
- (3) 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.

PART 13: OTHER INTERNAL CONTROL ARRANGEMENTS

69 Fraud prevention

An insurer must ensure that high standards of integrity apply to all aspects of its business, and must—

- (a) establish, implement and maintain adequate, appropriate and effective policies, procedures and internal controls, and allocate adequate and appropriate resources, to—
 - (i) deter, prevent, detect, record and, as required, promptly report any fraud it becomes aware of to the appropriate authorities; and
 - (ii) ensure that any fraud identified, which is within the scope of the insurer's corporate governance system, is remedied in a manner appropriate to the circumstances (including having regard to any relevant guidance provided by the police or other relevant authority);
- (b) assign operational responsibility for the insurer's fraud prevention and reporting to suitably senior officers or employees of the insurer;
- (c) provide counter-fraud training to its directors, senior managers and employees; and
- (d) ensure that the insurer's policies, procedures and internal controls, as referred to in sub-paragraph (a), form an integral part of the insurer's risk management system, including being taken account of in its internal audit programme.

70 Anti-money laundering and combating the financing of terrorism

An insurer must ensure that its measures in relation to anti-money laundering and combating the financing of terrorism form an integral part of the insurer's risk management system, including being taken account of in its internal audit programme.

71 Whistleblowing

An insurer must establish, implement and maintain an adequate and appropriate policy and procedures to encourage the reporting of any improper or unlawful behaviour, which must—

- (a) define the scope of improper or unlawful behaviour covered by the policy, including—
 - (i) failure to comply with the insurer'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 insurer's directors, senior managers and employees to raise concerns internally but outside of the normal management reporting structure, and include provisions requiring persons to whom it applies to raise their concerns directly with the Authority if they feel that they have not been adequately addressed internally;
- (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 ensuring confidentiality; and
- (e) be communicated effectively to all relevant persons to whom it applies.

PART 14: FAIR TREATMENT OF POLICYHOLDERS

72 Application of requirements (and class 12 requirement)

- (1) Subject to sub-paragraphs (2) to (5), paragraphs 73 and 74—
 - (a) apply to each of classes 1 to 9 insurance business written as direct insurance; and
 - (b) do not apply to reinsurance within classes 1 to 9, or to any of classes 10 to 12.

- (2) To avoid any doubt, despite the exclusion of any insurer from the requirements of paragraphs 73 and 74, the other requirements in the CGC applicable to the fair treatment of policyholders (and other stakeholders) still apply.
- (3) In respect of a class 12 insurer, every direct contract of insurance written by the insurer after the date on which the CGC came into operation which insures a person that—
 - (a) is not a related party of the insurer; and
 - (b) has not provided informed consent to the insurer in respect of that contract,in accordance with the Insurance Regulations 2021, must contain the information set out in sub-paragraph (5).
- (4) Any summary or confirmation of cover provided by a class 12 insurer, whether directly or indirectly, to a person in accordance with sub-paragraph (3) that has not already been provided with written information in accordance with sub-paragraph (5) relating to the contract in question, must also contain the information set out in sub-paragraph (5).
- (5) The information referred to in sub-paragraphs (3) and (4) must clearly and prominently—
 - (a) identify the insurer by its name as appearing on the register of authorised insurers under section 48 of the Act (if the insurer is using a business name in relation to the contract of insurance in question, the information must also state that name and explain that fact);
 - (b) state that the insurer is authorised by the Isle of Man Financial Services Authority; and
 - (c) state that the insurer is subject to a reduced level of regulation which may result in increased risk to any party insured under the contract.

73 Policyholders

- (1) An insurer must establish, implement and maintain adequate, appropriate and effective policies, procedures and internal controls that are integral to its corporate culture to ensure that its policyholders are treated fairly. This includes training where necessary to ensure compliance with those policies and procedures, where relevant, by the insurer's directors, senior managers, employees and other persons appointed to act for or on behalf of the insurer.
- (2) The policies, procedures and internal controls referred to in sub-paragraph (1) must, at a minimum, include—

- (a) ensuring that any conflicts of interest relevant to advice given to policyholders by or on behalf of the insurer are properly managed;
- (b) 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;
- (c) ensuring that any advice given to policyholders by or on behalf of the insurer is appropriate to their disclosed circumstances;
- (d) 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—
 - (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;
- (e) 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;
- (f) ensuring that private information about its policyholders is protected in accordance with applicable legal and regulatory requirements;
- (g) ensuring that the insurer deals with claims and complaints effectively and in a timely and fair manner through an easily understood, well disclosed, easily accessible and equitable process; and
- (h) 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.

74 Member policyholders and participating policyholders

Where an insurer has member policyholders or participating policyholders it must 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.

PART 15: INTERACTION WITH THE AUTHORITY

75 Communication and reporting

- (1) An insurer must—
 - (a) maintain open, honest and timely communications with the Authority, including communicating with the Authority as required and meeting with the Authority 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, appropriate and effective systems and internal controls to ensure that any information it provides to the Authority, and any other regulatory body to which the insurer is accountable, is appropriate, timely and effective.
- (2) An insurer must report to the Authority in writing anything relating to the insurer of which the Authority would reasonably expect notice, having regard to its regulatory objectives as set out in section 2(2) of the Financial Services Act 2008, including—
 - (a) any change or incident that could materially impact, currently or prospectively—
 - (i) its risk profile;
 - (ii) its financial condition, including its capital adequacy, liquidity adequacy or compliance with its regulatory capital requirement; or
 - (iii) the fair treatment of its policyholders; and
 - (b) any reportable matters as may be published as guidance by the Authority on its website for the purposes of this paragraph and updated from time to time,

as soon as is reasonably practicable after becoming aware of any such matter (or such other timescale as the Authority may specify in a publication referred to in sub-paragraph (b)) and, at the same time or in a timely manner subsequently, inform the Authority of the background of the matter, what action the insurer has taken or proposes to take (as applicable) and relevant timeframes.

PART 16: INTERPRETATION

76 Meaning of terms

- (1) In the CGC—

“**the Act**” means the Insurance Act 2008;

- “**actuarial function**”, in relation to an insurer, includes its appointed actuary (where applicable);
- “**ALM**” is an abbreviation of “asset-liability management” and, in relation to an insurer, refers to the practice of the insurer 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 insurer’s corresponding risk exposures;
- “**appointed actuary**” means the person appointed as actuary to the insurer in accordance with section 18 of the Act;
- “**audited accounts**”, in relation to an insurer, mean the audited annual accounts required to be produced to the Authority under section 14(3) of the Act and regulation 6 of the Insurance Regulations 2021;
- “**board**”, in relation to an insurer, means the board of directors of the insurer or, where the insurer has no board of directors, its equivalent governing body (for example, where the insurer is a limited partnership, its equivalent governing body is collectively its general partners);
- “**business plans**”, in relation to an insurer, mean the detailed activity plans and financial projections of the material operations of the insurer;
- “**capital adequacy**”, in relation to an insurer, means its compliance with paragraph 11(a);
- “**capital adequacy requirement**” means the requirement under paragraph 11(a);
- “**CGC**” is an abbreviation of “Corporate Governance Code of Practice for Insurers 2021”, as referred to in paragraph 1;
- “**class**”, in relation to an insurer or insurance business, has the meaning as given in regulation 3(3) of the Insurance Regulations 2021;
- “**compliance function**” has the meaning as given in paragraph 52;
- “**derivative**” means a financial asset or liability whose value depends on, or is derived from, other underlying factors, such as—
- (a) assets;
 - (b) liabilities;
 - (c) interest rates;
 - (d) currency exchange rates; or
 - (e) indices,
- and includes forwards, futures, options, warrants, swaps, and other financial instruments that have a similar economic effect;
- “**director**”, in relation to an insurer that is a limited partnership, means a general partner of the insurer;
- “**dormant**”, in relation to an insurer, has the meaning as given in regulation 18(2) of the Insurance Regulations 2021;

“**economic capital needs**”, in relation to an insurer, means the overall amount of financial resources necessary to adequately fund its current business and prospective business as determined by a comprehensive financial assessment (consistent with the relevant requirements of Schedule 2) of the cost of running that business, including taking account of—

- (a) its business plans and risk appetite, limits and tolerances;
- (b) maintaining compliance with its regulatory capital requirement;
- (c) its risks;
- (d) the relationship between those risks; and
- (e) the risk mitigation measures it has in place, including the likely timing and effectiveness of any potential actions its management would take if needed;

“**ERM**” is an abbreviation of ‘enterprise risk management’ and has the meaning given in paragraphs 60(e) to 66;

“**external auditor**”, in relation to an insurer, means the insurer’s auditor appointed under section 15 of the Act;

“**financial management**”, in relation to an insurer, means its management activity for the purpose of ensuring it complies with its capital adequacy requirement and liquidity adequacy requirement;

“**forecast time horizon**” has the meaning given in paragraph 2(2) of Schedule 2;

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

“**function**”, in relation to an insurer, refers to the activities of the insurer that are associated with a function of the insurer or the means (including systems and resources) by which the insurer carries out the function, or both, as the context requires, and where the terms activity and function are used together in respect of a requirement (such as in connection with outsourcing and delegation), this is to avoid any doubt that all relevant matters are included in the requirement and not just those associated with the functions specified in the CGC;

“**group**”, in relation to an insurer, means—

- (a) the insurer; or
- (b) where the insurer is a limited partnership, its partners; and
- (c) any other legal person which is a—
 - (i) subsidiary; or
 - (ii) holding company,of a person in accordance with sub-paragraph (a) or (b), and any subsidiary of that holding company;

“**holding company**” has the meaning given in section 220 of the Companies Act 2006;

“**implement**”, in relation to a requirement, does not limit appropriate delegation in relation to the requirement;

“**independent non-executive director**”, in relation to an insurer, means a director of the insurer who—

- (a) apart from his or her—
 - (i) directors’ fees in respect of his or her position as a director of the insurer; and
 - (ii) subject to sub-paragraph (b)—
 - (A) other benefits attributable to his or her position as a director of the insurer; and
 - (B) shareholdings in relation to the insurer or its group, as may be applicable, is independent of the group (as applicable) and management of the insurer; and
- (b) is free from any relationships or circumstances which could materially interfere with the exercise of his or her independent judgment in relation to the affairs of the insurer;

“**insurer**” means a person to whom the CGC applies in accordance with paragraph 5(1);

“**internal audit function**” has the meaning as given in paragraph 48;

“**liquidity adequacy**”, in relation to an insurer, means its compliance with paragraph 11(b);

“**liquidity adequacy requirement**” means the requirement under paragraph 11(b);

“**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);

“**ORSA**” is an abbreviation of ‘own risk and solvency assessment’ and, in relation to an insurer, means the process described in Schedule 2;

“**outsourced activity or function**”, in relation to an insurer, refers to an activity or function of the insurer that is carried out by a person external to the insurer;

“**outsourced provider**”, in relation to an insurer, refers to a person external to the insurer (whether within or external to the insurer’s group) that carries out an outsourced activity or function of the insurer;

“**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 or compensated under that policy, gives the policyholder a right to participate in the profits of the insurer;

“**permit holder**” means a person that is the holder of a permit under section 22 of the Act;

- “**policyholder**” has the meaning as given in section 54 of the Act, and includes prospective policyholders of the insurer as the context requires;
- “**procedures**”, in relation to an insurer and without limiting any other requirement in relation to processes, also include any processes necessary for the implementation of the insurer’s strategies and policies;
- “**recovery scenarios**” are as referred to in paragraph 11(c);
- “**registered insurance manager**” means a person registered as an insurance manager under Part 6 of the Act;
- “**regulatory capital requirement**”, in relation to an insurer, means the greater of its minimum capital requirement (“MCR”) and solvency capital requirement (“SCR”) in accordance with the—
- (a) Insurance (Long-Term Business Valuation and Solvency) Regulations 2021; or
 - (b) Insurance (Non Long-Term Business Valuation and Solvency) Regulations 2021,
- (as applicable) and regulatory capital shall be construed accordingly;
- “**risk appetite**” has the meaning given in paragraph 64(1)(a);
- “**risk appetite framework**” has the meaning as set out in paragraph 64;
- “**risk capacity**” has the meaning given in paragraph 64(2);
- “**risk limits**” has the meaning given in paragraph 64(1)(b)(i);
- “**risk profile**”, in relation to an insurer, means the particular range and significance of risks to which the insurer is or may be exposed;
- “**risk tolerances**” has the meaning given in paragraph 64(1)(b)(ii);
- “**senior management**”, in relation to an insurer, means any person whose appointment is required to be notified to the Authority 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 Authority under the Act other than as a controller;
- “**senior manager**”, in relation to an insurer, means a member of its senior management;
- “**shareholders**”, in relation to an insurer, mean the owners of the insurer including (as applicable)—
- (a) the owners of its shares;
 - (b) its members (if the insurer is a mutual or similar);
 - (c) its partners (if the insurer is a partnership); and

(d) its member policyholders and participating policyholders, or their equivalents;

“**stakeholder**”, in relation to an insurer, means any person with a direct or indirect interest or involvement (a stake) in the insurer because that person can affect or be affected by the insurer’s actions, strategies, policies or procedures (an insurer’s stakeholders include where applicable, its policyholders, shareholders and other investors, creditors, employees, the general public, the Isle of Man Government and the Authority);

“**subsidiary**” has the meaning given in section 220 of the Companies Act 2006;

“**technical provisions**” has the meaning given in regulation 3(1) of the Insurance Regulations 2021; and

“**written**” has the meaning given in regulation 3(1) of the Insurance Regulations 2021.

ISSUED 2 DECEMBER 2021

SCHEDULE 1 (RISKS)

[Paragraph 60(b)]

1 General

Without limiting any other requirement in the CGC, an insurer must apply the guidance within this Schedule as is applicable to the insurer.

The risks referred to in this Schedule are not intended to be, and must 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.

2 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 must apply the following guidance:

- (1) An insurer must establish, implement and maintain strategic underwriting and pricing policies within its ERM framework based on sound methodology and reasonable assumptions that are approved, monitored and reviewed by its board, which address the—
 - (a) insurer's underwriting risk according to the insurer's risk appetite framework including its relevant component risk limits structure;
 - (b) nature of the risks to be undertaken by the insurer; and
 - (c) interaction of the underwriting strategy with the insurer's reinsurance strategy (and any other risk transfer mechanism of the insurer) and the pricing of its insurance products.
- (2) An insurer must 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.
- (3) An insurer must establish, implement and maintain systems to control all of the claims and other obligations and expenses referred to in subparagraph (2), and those systems must be monitored on an ongoing basis by its senior management and properly overseen by its board.
- (4) An insurer must have a clear strategy to mitigate, and where appropriate diversify, the underwriting risks to which it is or may be 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 complying with its capital adequacy requirement, liquidity adequacy requirement and regulatory capital requirement. This strategy must be an integral part of the insurer's underwriting policy that is approved, monitored and reviewed by its board.

- (5) An insurer must 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 –
 - (a) ensuring that its reinsurance programme is appropriate to its risk profile and provides coverage which, after taking into account the real transfer of risk, enables the insurer to comply with its capital adequacy requirement, liquidity adequacy requirement and regulatory capital requirement; and
 - (b) taking all reasonable steps to ensure that the protection provided by its reinsurers is secure.
- (6) In addition to sub-paragraph (5), an insurer must 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 comply with its capital adequacy requirement, liquidity adequacy requirement and regulatory capital requirement.
- (7) An insurer must ensure that all of its risk transfer mechanisms are properly accounted for so that the insurer's financial statements meet the presentational requirements (such as being true and fair, or similar, as applicable) of the accounting standards adopted by the insurer in accordance with regulation 6(4) of the Insurance Regulations 2021.
- (8) An insurer, in respect of its risk transfer mechanisms, must promptly document the principal economic and coverage terms and conditions agreed upon by the parties involved and finalise an adequate, appropriate and effective corresponding formal contract in a timely fashion.

3 Insurance provisions risk

Insurance provisions risk, in relation to an insurer, refers to the possibility that the insurer's technical 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's policy for establishing and maintaining its technical provisions must, amongst other things, take into account the potential for unexpected or atypical claims and expense occurrence and catastrophe events that might adversely affect the insurer. This includes, where appropriate, using suitable techniques (as referred to in paragraph 62(2)) across an appropriate range of adverse scenarios in order to assess its capital adequacy, liquidity adequacy

and compliance with its regulatory capital requirement, such that should its technical provisions need to be increased it has sufficient capital or, where appropriate, other financial resources to do so.

4 Investment risk

Investment risk, in relation to an insurer, encompasses the various risks to which the insurer is or may be exposed in relation to its investment activities.

Investment risks may include credit risk, market risk, liquidity risk and custody risk. These and other component risks are described further in this schedule.

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

- (1) An insurer must only invest in assets where the insurer is able to properly manage the risks involved and properly assess its economic capital needs, capital adequacy, liquidity adequacy and regulatory capital compliance.
- (2) An insurer must establish, implement and maintain an overall strategic investment policy within its ERM framework that addresses the following elements (as applicable)—
 - (a) specifying the nature, role and extent of the insurer's investment activities such that, in maintaining its regulatory capital, it takes account of the capital implications as a consequence of its investments in accordance with the—
 - (i) Insurance (Non Long-Term Business Valuation and Solvency) Regulations 2021; or
 - (ii) Insurance (Long-Term Business Valuation and Solvency) Regulations 2021,as applicable;
 - (b) setting out explicit risk management procedures within the investment policy 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;
 - (c) the insurer's risk profile;
 - (d) the investment policy's relationship with the insurer's ALM policies;
 - (e) the insurer's investment risks according to its risk appetite framework, including its component risk limits structure within its risk management policies;
 - (f) the determination of the strategic asset allocation, that is, the long-term asset mix over the main investment categories;
 - (g) the establishment of limits for asset allocation by geographical area, markets, sectors, counterparties and currency;

- (h) the extent to which the holding of some types of assets is restricted or prohibited;
 - (i) the conditions under which the insurer can pledge or lend assets;
 - (j) limits of delegated authority to make or alter the insurer's investments;
 - (k) clear accountability in respect of all of its asset transactions and associated risks; and
 - (l) where the insurer is using or intending to use derivatives, an overall policy on their use.
- (3) An insurer's risk management system must, amongst other things, cover the risks associated with its investment activities that might affect the coverage of its technical provisions or its compliance with its capital adequacy requirement, liquidity adequacy requirement or regulatory capital requirement.
- (4) An insurer must 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 10. These must ensure that investment procedures are documented and properly overseen. Where appropriate, the functions responsible for measuring, monitoring, settling and controlling asset transactions must be separate from the insurer's front office functions.
- (5) The board of an insurer must retain ultimate oversight of, and ensure clear management accountability for, the insurer's investment policies and procedures.
- (6) The board of an insurer must ensure that any persons involved with an insurer's significant investment activities have the appropriate integrity, competence, experience and qualifications for their respective roles in relation to the insurer.
- (7) An insurer must have rigorous audit procedures that include full coverage of its investment activities to ensure the timely identification and reporting of weaknesses in the insurer's internal controls and procedures and any other operating system deficiencies. If the audit is carried out internally it must be appropriately independent of the function being reviewed.
- (8) An insurer must establish, implement and maintain contingency plans to mitigate the effects of deteriorating investment conditions.

5 ALM

- (1) An insurer must establish, implement and maintain an ALM system (as part of its ERM framework) including policies and procedures to ensure

on an ongoing basis that its investment activities and asset positions are appropriate to its risk profile (including its liability profile). The insurer must, within its risk management system, take account of the risks associated with mismatches between its assets and liabilities.

- (2) An insurer's ALM policies must clearly specify the nature, role and extent of its ALM activities and their relationship with its product development, pricing functions and investment management.

6 Derivative risk

Derivative risk, in relation to an insurer, refers to the risks to which the insurer is or may be exposed in relation to its use of derivatives.

Without limiting the investment risk guidance given above, in managing this risk an insurer must apply the following guidance:

- (1) An insurer may only use derivatives for the purpose of reducing the insurer's risks or to facilitate efficient portfolio management in respect of its investments.
- (2) In sub-paragraph (1) "efficient portfolio management", in relation to an insurer, includes that the insurer must only make investments that are economically appropriate for the insurer and consistent with the sound and prudent management of its business. Accordingly, appropriate uses may include reducing the insurer's risks or costs, or the generation of capital or income for the insurer that is appropriate to its business and consistent with it having in place effective risk management (including ALM) and financial management. Appropriate uses do not include speculative uses.
- (3) The board of an insurer that uses, or intends to use, derivatives must—
 - (a) 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 insurer;
 - (b) ensure that any persons conducting and monitoring the derivative activities of the insurer have the appropriate integrity, competence, experience and qualifications for their respective roles in relation to the insurer;
 - (c) establish, implement and maintain appropriate arrangements to verify pricing of its derivatives independently if not quoted on a recognised exchange;
 - (d) ensure that the insurer has employees with appropriate skills to effectively vet models used by its front office (as applicable) and to price the instruments used, the board must also ensure that that pricing follows market convention and that those functions are separate from the insurer's front office; and

- (e) establish, implement and maintain a risk management system (as part of its overall risk management system) in relation to its use of derivatives, including internal control system and sufficient personnel and resources consistent with sub-paragraph (6).
- (4) An insurer using, or intending to use, derivatives must establish implement and maintain an appropriate policy for their use in relation to the insurer that must be approved, monitored and reviewed by its board. This policy must be consistent with the insurer's activities, its overall strategic investment policy, ALM strategy and its risk appetite framework established by its board. The policy must address at least the following elements –
- (a) the purposes for which derivatives can be used;
 - (b) the establishment of appropriately structured exposure limits for derivatives taking into account the purpose of their use and their associated risks;
 - (c) restrictions on the holding of certain types of derivatives; and
 - (d) appropriate divisions of responsibility and a framework of accountability for derivative transactions.
- (5) An insurer using, or intending to use, derivatives must ensure its risk management system encompasses its risks from derivative activities so that the risks arising from all derivative transactions undertaken by the insurer can be –
- (a) analysed and monitored individually and in aggregate; and
 - (b) 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.
- (6) An insurer using, or intending to use, derivatives must 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 insurer's policies and procedures, and with its legal and regulatory obligations as identified in accordance with paragraph 10. Those controls must ensure appropriate segregation between individuals who measure, monitor, settle and control derivatives and individuals who initiate transactions.
- (7) Where applicable, the internal audit function of an insurer that uses, or intends to use, derivatives, must establish, implement and maintain rigorous procedures that include coverage of its derivative activities to ensure the timely identification and reporting of weaknesses in the insurer's internal controls and procedures, and any other operating system deficiencies. If the audit is carried out internally it must be appropriately independent of the function being reviewed.

7 Market risk

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

The significance of market risk to the insurer 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 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 insurer'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.

8 Credit risk

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

Credit risk includes the insurer's exposure to—

- (a) default (counterparty) risk – the risk that the insurer 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 insurer's increased exposure to losses due to concentration of its credit exposures, including

exposures in a geographical area, economic sector, or with a single counterparty or connected parties.

9 Liquidity risk

Liquidity risk, in relation to an insurer, refers to the possibility that the insurer, 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—

- (a) mismatches between the size and timing of the insurer's asset and liability cash flows;
- (b) associated investment risk – the risk that an investment by the insurer in a member of the insurer's group or other associate of the insurer might be difficult to sell, or that greater credit risk is accepted by the insurer 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 insurer might create a drain on the financial or operating resources of the insurer;
- (c) funding risk – the risk that the insurer 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 insurer 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 deterioration in the economy, abnormally volatile or stressed markets or political and legal risk.

10 Operational risk

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

11 Group risk

Group risk includes the risk that the insurer may be adversely affected by a financial or non-financial occurrence relating to another legal entity that is part of its group. For example—

- (a) losses or illiquidity affecting other parts of the group creating pressure to divert financial resources to those parts and depleting the resources available to the insurer;
- (b) group restructuring having a negative risk impact on the insurer;
- (c) risks arising from contagion, leveraging, double or multiple gearing, concentration, large exposures or complexity, which may be relevant to intra-group transactions and arrangements such as participations, loans, other outstanding balances, guarantees and outsourcing; or
- (d) where the group operates a more centralised corporate governance system and the insurer places a degree of reliance on that system, risks may arise from group-wide risk management strategies, policies, systems or functions if these do not have a risk focus or materiality level that is appropriate for the insurer's own risk management purposes.

12 Business market and environment risk

Business market and environment risk, in relation to an insurer, refers to the possibility of an adverse impact on the insurer resulting from external threats. Adverse business conditions can arise from various sources or combination of sources, including—

- (a) political, legislative, economic, environmental, health, sociological and technological factors; and
- (b) policyholders, outsourced providers, key business counterparties and competitors.

13 Business planning risk

Business planning risk, in relation to an insurer, refers to the possibility of an adverse impact on the insurer 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.

14 Information technology and communication technology risk

Information technology and communication technology risk, in relation to an insurer, refers to the possibility of an adverse impact on the insurer resulting from failure, unauthorised or erroneous use, or other interruption in operation of its information technology and communication technology systems.

15 Business continuity and disaster risks

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

16 Legal and compliance risk

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

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

17 Crime and fraud risk

Crime and fraud risk, in relation to an insurer, refers to the possibility of the insurer (including its directors, senior managers, employees and other persons appointed to act on behalf of the insurer) being involved in criminal or civil wrongdoing.

18 Reputational risk

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

19 Strategic risk

Strategic risk, in relation to an insurer, refers to the possibility of an adverse impact on the insurer or its stakeholders due to factors such as poor business objectives, substandard execution of decisions, inadequate or inappropriate resource allocation or failure to understand and respond appropriately to changes in its internal and external risk environment.

SCHEDULE 2 (ORSA)

[Paragraph 60(e)(i)]

1 ORSA requirement

An insurer must establish, implement and maintain an ORSA process and supporting framework consistent with this Schedule which is adequate and appropriate to the nature, scale and complexity of the insurer, its activities and the risks to which it is or may be exposed.

2 General

- (1) An insurer must carry out an ORSA at appropriate intervals (including as referred to in sub-paragraph (3)) and at least annually, to assess—
 - (a) the adequacy of its risk management;
 - (b) its compliance, including on a continuous basis over an appropriate forecast time horizon, with its—
 - (i) regulatory capital requirement; and
 - (ii) capital adequacy requirement and liquidity adequacy requirement: and
 - (c) the significance with which its risk profile deviates from the assumptions underlying its regulatory capital requirement.
- (2) Pursuant to sub-paragraph (1)(b), the forecast time horizon must be a period that is—
 - (a) appropriate to the nature of the insurer's risk profile and business planning period; and
 - (b) at least 3 years subject to the Authority's agreement in writing to a shorter period.
- (3) An insurer must, in a timely manner, perform an ORSA at any point where the risk profile of the insurer has deviated significantly from the assumptions underlying the previous ORSA it has carried out.

3 Responsibility and communication

- (1) An insurer's board and senior management are responsible for its ORSA.
- (2) An insurer's board must take an active part in the insurer's ORSA, including steering how the assessment is to be performed, challenging results and approving significant matters in relation to the ORSA.
- (3) Appropriate information in respect of an insurer's ORSA, including at a minimum its results and conclusions, must be communicated in a timely and appropriate manner to all relevant persons working for or on behalf

of the insurer once the process and results of the ORSA have been approved by its board.

- (4) Subject to sub-paragraph (5), an insurer must, as soon as is reasonably practicable, inform the Authority of the results of each ORSA it carries out. The results include the report referred to in paragraph 9(c) and any other information as the Authority may specify.
- (5) An insurer, in accordance with such approval, is exempt from the requirement in sub-paragraph (4) if it has obtained the Authority's written approval to be so.

4 Integration

An insurer must—

- (a) ensure that its ORSA is an integral part of its business strategy and strategic decisions; and
- (b) take account of the results of its ORSA and the insights gained during its ORSA process in at least its risk management, financial management, business planning and product development and design.

5 Policy

An insurer must establish, implement and maintain an ORSA policy which includes at least an adequate and appropriate description of—

- (a) the processes and procedures required to conduct its ORSA;
- (b) the roles and responsibilities of persons relevant to its ORSA;
- (c) the link between the insurer's risk profile, its risk appetite framework and its overall economic capital needs; and
- (d) the methods to be used in its ORSA process and procedures including information on—
 - (i) the recognition and valuation bases to be used;
 - (ii) how and how often stress tests, sensitivity analyses, reverse stress tests and other relevant analyses are to be performed;
 - (iii) data quality;
 - (iv) the frequency with which the ORSA itself will be performed and the justification for that frequency; and
 - (v) the timing of the performance of its ORSA and the circumstances which would trigger the need for an ORSA outside of these regular timescales.

6 Methods, assumptions and coordination of relevant factors

An insurer's ORSA must—

- (a) encompass and suitably categorise all of the reasonably foreseeable, relevant and material risks to which the insurer is or may be exposed, whether quantifiable or not, including any off-balance sheet risks (risks include those referred to in Schedule 1);
- (b) consider its forecast time horizon;
- (c) take account of potentially relevant and material changes in the insurer's risk profile and the relevant and material factors likely to affect its future risk profile during its forecast time horizon, including—
 - (i) its business strategies and plans;
 - (ii) its risk management and internal control systems (including notably, its risk appetite framework);
 - (iii) the timing and effect of management actions it might reasonably expect to take if necessary to mitigate its risks; and
 - (iv) its economic and financial environment, including any factor affecting its operational risks;
- (d) consider the impact of a range of plausibly adverse scenarios in the medium and longer term business strategy of the insurer;
- (e) include recognition and valuation bases that are appropriate to the insurer's business and risk profile, which support the consistent reporting of the economic reality of the insurer's risk profile and financial condition;
- (f) include processes and techniques consistent with paragraph 62(2);
- (g) where a risk of the insurer is plausibly relevant and material, but is not practicably quantifiable, make a qualitative assessment that is appropriate to the risk and sufficiently detailed to be useful for the insurer's risk management and financial management purposes;
- (h) identify the relationship between its risk management and the quantity, quality and liquidity of the financial resources it needs (its economic capital needs) and has available;
- (i) take account of the quantity, quality and composition of its own funds to meet its regulatory capital requirement (including across relevant tiers and how the composition may change as a result of redemption, repayment, maturity or other factor);
- (j) take account of the quantity, quality and composition of any additional capital and other financial resources it has available (including how the composition may change as a result of redemption, repayment, maturity or other factor) to meet any additional economic capital needs it has remaining after meeting its regulatory capital requirement and allowing for the effectiveness of its applicable controls to mitigate its risks; and

- (k) take account of the availability and liquidity of its financial resources to meet its expected money outflows and potential for large, unexpected money outflows.

7 Differences between economic capital needs and regulatory capital requirement

An insurer must as part of its ORSA –

- (a) assess whether its risk profile deviates from the assumptions underlying the regulatory capital requirement calculation and quantitatively estimate any material impact on its economic capital needs assessment due to such deviation (in assessing the materiality of a deviation, if an adequate, appropriate and demonstrable qualitative analysis indicates on a reasonably prudent basis that it is not material then a quantitative assessment is not required);
- (b) if it uses recognition or valuation bases in its ORSA that are different to corresponding regulatory capital requirement bases –
 - (i) explain how the use of those different bases ensure better consideration of the specific risk profile of the insurer, while complying with the requirement for sound and prudent management; and
 - (ii) quantitatively estimate the impact on the economic capital needs assessment due to the use of those different bases instead of the bases used in the regulatory capital requirement.

8 Results, conclusions and additional information

- (1) An insurer must as part of its ORSA –
 - (a) assess the adequacy of its risk management;
 - (b) determine its economic capital needs as well as analyse its financial position and ability to comply with its capital adequacy requirement and its regulatory capital requirement on a continuous basis over its forecast time horizon;
 - (c) assess the quality, adequacy and composition of its own funds to meet its regulatory capital requirement (including across relevant tiers) on a continuous basis over its forecast time horizon;
 - (d) assess the quality, adequacy and composition of its other capital and other financial resources (as applicable) to meet its additional capital required to address its economic capital needs (as applicable) on a continuous basis over its forecast time horizon;

- (e) assess the availability and liquidity of its financial resources to meet its liquidity adequacy requirement on a continuous basis over its forecast time horizon;
 - (f) identify and explain how any plausibly relevant and material risks to which it is or may be exposed, that are not practicably quantifiable, are addressed within its risk management and financial management policies (as applicable); and
 - (g) compile qualitative information on and, where material deviations have been identified, quantification of the extent to which the insurer's risks are not reflected in the calculation of its regulatory capital requirement (as applicable).
- (2) An insurer, in considering within its ORSA its regulatory capital compliance over its forecast time horizon and in respect of the technical provisions it is required to calculate as part of its regulatory capital requirement calculation, must require its actuarial function (if it is required to have an actuarial function) to—
- (a) provide input as to whether the insurer would be in a position to comply continuously with the requirements regarding the calculation of its technical provisions; and
 - (b) identify risks arising from the uncertainties connected to that calculation.
- (3) Subject to sub-paragraph (4), in relation to an insurer carrying on business within classes 3 to 9 or 11 (or any combination thereof), the Authority may modify (including reduce) in writing some or all of the requirements of sub-paragraph (2) where the Authority considers it appropriate to do so.
- (4) Where considering a reduction in requirement as referred to in sub-paragraph (3) in relation to an insurer, the Authority may require the insurer to show to the Authority's satisfaction why the actuarial requirements in question warrant such reduction.

9 Records

An insurer's ORSA must be supported by suitable evidence and documentation, including its—

- (a) ORSA policy (including the matters referred to in paragraph 5);
- (b) record of each ORSA (including the matters referred to in paragraphs 6 and 7 and paragraph 8(2)); and
- (c) report for each ORSA (including the matters referred to in paragraph 8, as applicable).

10 Modifications to this schedule for class 12 insurers

- (1) A class 12 insurer in respect of this schedule is exempt from the following paragraphs but, where applying such an exemption, must apply the alternative requirement shown (as applicable)—
 - (a) paragraph 2(1)(c);
 - (b) subject to sub-paragraph (2), paragraph 2(2)(b) and instead must apply an appropriate forecast time horizon which is at least 1 year;
 - (c) paragraph 3(4) and instead must—
 - (i) provide a summary ORSA return in accordance with Schedule 4; and
 - (ii) hold the report referred to in paragraph 9(c) available to submit to the Authority in a timely manner if required;
 - (d) paragraph 7; and
 - (e) paragraph 8(1)(g).
- (2) Sub-paragraph (1)(b) applies only to a class 12 insurer that is dependent upon the group to which it belongs for new or renewal business (as the case may be) in circumstances where the nature and extent of its overall prospective business profile is not sufficiently foreseeable to be meaningfully forecast 3 years in advance.

SCHEDULE 3 (DIRECTORS' CERTIFICATE ON CORPORATE GOVERNANCE)

[Paragraph 8]

To the Isle of Man Financial Services Authority

(State the name of the insurer for which this certificate is given (herein the “insurer”))

We certify that:

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

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

(State name and position held within the insurer)

The report referred to above must include—

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

SCHEDULE 4 (SUMMARY ORSA RETURN)

[Paragraph 10(1)(c)(i) of Schedule 2]

- (1) A summary ORSA return, as referred to in paragraph 10(1)(c)(i) of Schedule 2 must—
 - (a) contain such information as may be specified by the Authority from time to time (which includes modifying the information referred to in paragraph (2));
 - (b) be in such form as is required by the Authority; and
 - (c) be submitted electronically unless the Authority requires otherwise.
- (2) Pursuant to 10(1)(c)(i) of Schedule 2 and paragraph (1), a summary ORSA return must include the following—
 - (a) the insurer's name;
 - (b) the ORSA's forecast time horizon and, if less than 3 years, the rationale for the period chosen;
 - (c) the reason the ORSA was carried out;
 - (d) the date the ORSA was completed;
 - (e) who carried out the ORSA work;
 - (f) who/what body provided ultimate approval of the ORSA;
 - (g) such information as is required by the Authority in relation to any or all of the following—
 - (i) the insurer's immediate and (if different) longer term business goals;
 - (ii) the insurer's current and prospective regulatory capital requirement;
 - (iii) the insurer's current and prospective economic capital needs;
 - (iv) any dividends or distributions the insurer is planning to make;
 - (v) the insurer's own funds;
 - (vi) any other on- or off- balance sheet financial resources of the insurer;
 - (vii) any recapitalisation options available to the insurer (if needed);
 - (viii) confirmation that the insurer continues at all times to meet its current and prospective—
 - (A) regulatory capital requirement;

- (B) capital adequacy requirement; and
- (C) liquidity adequacy requirement; and
- (ix) such other information as the Authority may require (including in respect of the insurer, its risks, operations, business or any relevant and foreseeable significant events).

ENDNOTES

Table of Endnote References

¹ The format of this legislation has been changed as provided for under section 75 of, and paragraph 2 of Schedule 1 to, the Legislation Act 2015. The changes have been approved by the Attorney General after consultation with the Clerk of Tynwald as required by section 76 of the Legislation Act 2015.