ANNEX

DRAFT FOR CONSULTATION PURPOSES ONLY

GUIDELINE
ON
ENTERPRISE RISK MANAGEMENT

Insurance Authority

1. Introduction

1.1 This Guideline is issued by the Insurance Authority ("IA") pursuant to section 133 of the Insurance Ordinance (Cap. 41) ("Ordinance") and its principal function to regulate and supervise the insurance industry for the protection of existing and potential policy holders. This Guideline also takes into account the relevant Insurance Core Principles, Standards, Guidance and Assessment Methodology ("ICPs") promulgated by the International Association of Insurance Supervisors ("IAIS"), in particular:

- ICP 8 stipulates that insurers should have, as part of their overall corporate governance framework, effective systems of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters and internal audit; and

- ICP 16 stipulates that insurers should establish an enterprise risk management ("ERM") framework for solvency purposes to identify, measure, report, monitor and manage the insurers' risk exposure in an ongoing and integrated manner.

1.2 The main objective of this Guideline is to nurture a sound risk culture in the insurance industry that would be reflected in the values, attitudes and norms of business behaviour. The board of directors ("Board") and senior management of an authorized insurer should take ownership for shaping a sound risk culture to drive the insurers' business practices and decisions.

1.3 The risk-based capital regime ("RBC regime") for Hong Kong's insurance industry is to comprise of three key components, commonly known as the "Three Pillars". Pillar 1 covers the regulatory capital rules and requirements; Pillar 2 covers corporate governance and ERM; and Pillar 3 covers reporting and disclosure requirements.

1.4 This Guideline sets out the Pillar 2 requirements which provide the impetus for authorized insurers to (a) put in place a robust system of risk governance; (b) proactively identify and assess their risk exposure; (c) maintain sufficient capital to cover risks not captured or not adequately captured under Pillar 1; and (d) develop and enhance risk management techniques in monitoring and managing these risk exposure.

1.5 This Guideline also sets out the supervisory objectives, guidance, and expectations of the IA for assessing the overall competence and effectiveness of an authorized insurer's ERM framework and Own Risk and Solvency Assessment ("ORSA"). Authorized insurers should take into account this Guideline and the nature, scale and complexity of risks associated with their business operations in Hong Kong and with the operations of their groups when establishing and maintaining their ERM framework and conducting ORSA.

1.6 A principles-based approach is adopted for this Guideline as follows. The primary focus is to ensure that the ERM framework and the ORSA adopted by an authorized insurer achieve the objectives stated in sections 3 to 9 of this Guideline[1]. An authorized insurer may consider adopting other appropriate ways to achieve the objectives. However, the IA expects the authorized insurer to be able to explain (to the IA's satisfaction) how it has diverged from any specified requirement in sections 3 to 9 of this Guideline, as it applies to the insurer's ERM framework or ORSA, and why (despite such divergence) the objectives are still achieved.

1.7 Unless otherwise specified, words and expressions used in this Guideline shall have the same meanings as given to them in the Ordinance.

1.8 This Guideline does not have the force of law and should not be interpreted in a way that would override the provision of any law. A non-compliance with the provisions in this Guideline would not by itself render an authorized insurer liable to judicial or other proceedings. A non-compliance may, however, reflect on the IA's view of the continued fitness and properness of the directors or controllers of authorized insurers to which this Guideline applies. The IA may also take guidance from this Guideline in considering whether there has been an act or omission likely to be prejudicial to the interests of policy holders or potential policy holders (albeit the IA will always take account of the full context, facts and impact of any matter before it in this respect). The IA reserves the right to review and update this Guideline from time to time as necessary.

[1] The objectives and outcomes in this respect are stated in the whole of the content of Section 3 and in each of the opening parts of Sections 4 to 9 under the heading "Objectives".

2. Application

2.1 Unless otherwise directed by the IA, this Guideline applies to all authorized insurers, except:

(a) those insurers which have ceased accepting new insurance business and are in the course of running off their liabilities with an insignificant run-off portfolio[2] in Hong Kong;

(b) Lloyd's;

(c) captive insurers; and

(d) marine mutuals,

where:

"Lloyd's" has the meaning assigned to it under section 2(1) of the Ordinance;

"captive insurer" has the meaning assigned to it under section 2(7) of the Ordinance; and

"marine mutual" refers to an authorized insurer which is a mutual company and insures only its members against losses, damages or liabilities arising from or in relation to marine adventure, and whose articles of association, rules or by-laws provide for calling for additional contributions from, or reduction of benefits to, its members.

2.2 The minimum requirements on the ERM framework *(section 6)* and the ORSA *(section 9)* shall apply to all authorized insurers (save for those exceptions set out in section 2.1 above).

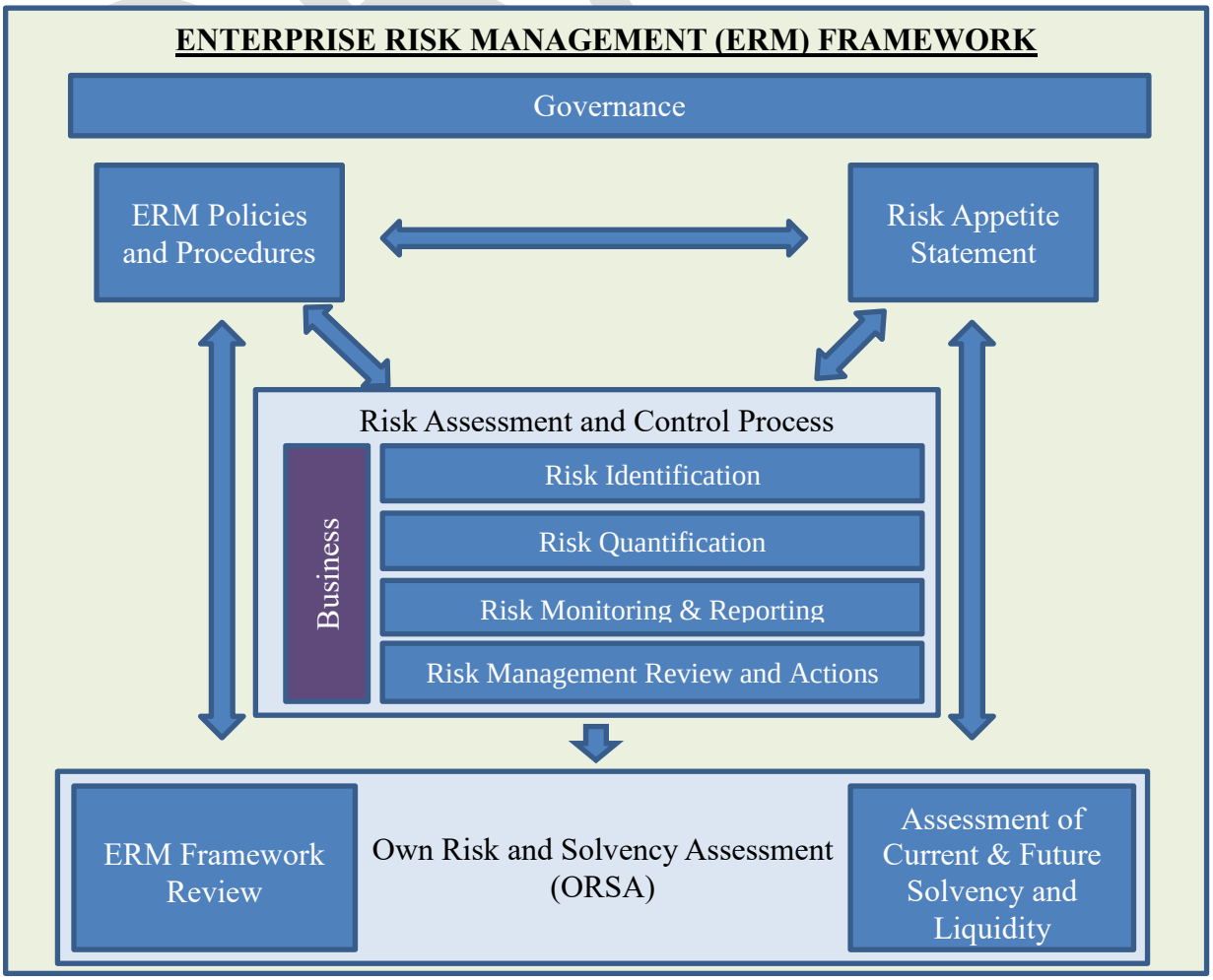
2.3 An authorized insurer may rely on the ERM framework or policies of the group to which it belongs provided that the ERM framework or policies of the group are appropriate and adequate for the nature, scale and complexity of the risks associated with its business operations in Hong Kong and the operations of the entire group and are in compliance of this Guideline. Otherwise, the authorized insurer should establish a designated local ERM framework and/or policies for its Hong Kong operations in accordance with this Guideline.

[2] The question of whether or not an authorized insurer's run-off portfolio in Hong Kong is considered "insignificant" shall be determined by the IA in consultation with the relevant insurer. The IA's determination as notified to the relevant insurer shall be final.

3. Overview of ERM Framework and General Requirements

3.1 ERM for solvency purposes is the coordination of risk management, strategic planning, capital adequacy and financial efficiency in order to enhance sound operation of the authorized insurer and ensure adequate protection of policy holders. An authorized insurer should establish an integrated set of processes and activities within its risk management system for the effective implementation of its ERM framework.

3.2 An authorized insurer needs to have in place an ERM framework with sufficient governance to ensure a safe and sound operation. An ERM framework is the process of identifying, assessing, measuring, monitoring, controlling and mitigating risks in respect of the insurer. It involves the authorized insurer setting its risk appetite and performing a self-assessment to determine all reasonably foreseeable and relevant material risks that the insurer faces, and the inter-relationships between those risks, providing a link between ongoing operational management of risk and longer-term business goals and strategies.



3.3 The Board of an authorized insurer has the ultimate responsibility for establishing, implementing and overseeing an effective ERM framework, which should consist of:

(a) an appropriate governance structure with well-defined roles and responsibilities and reporting lines in order to maintain a sound system of checks and balances *(see section 4)*;

(b) a risk appetite statement that articulates the level and types of risk that the insurer is willing to take to achieve its corporate objectives and business strategies *(see section 5)*;

(c) ERM policies and procedures that describe the governance structure of ERM across the business and describe how the authorized insurer:

- identifies risk;
- measures and quantifies risk;
- monitors and reports risk; and
- reviews risks and, where appropriate, takes actions to mitigate and/or transfer such risks.

The related risk assessment and control processes described should be performed on a regular basis. Such processes need to be further embedded in the business cycle and different business activities (e.g. underwriting, asset-liability management ("ALM"), investment, reinsurance, etc) and business planning *(see sections 6 and 7)*;

(d) a feedback loop mechanism that ensures continued effectiveness of the ERM framework *(see section 8)*; and

(e) conducting an ORSA on a regular basis to assess the insurer's current and future risk profile, solvency and liquidity positions, and to review the effectiveness of the ERM framework *(see section 9)*.

3.4 An authorized insurer's ERM framework needs to be:

(a) set at a level of sophistication that is commensurate with the nature, scale and complexity of the insurer and the risks it faces;

(b) coordinated with corporate objectives, strategic planning and management of regulatory capital requirements and capital needs, all of which should be linked to the risk appetite of the insurer;

(c) forward-looking with a reasonable time horizon (normally covering at least a three year projection) consistent with the nature of the risks, including risks pertaining to the group to which it belongs, that may affect the insurer's operations in Hong Kong and the insurer's business planning horizon;

(d) able to address material risks[3] and their correlations, and the potential impact on the insurer's business;

(e) adopting a transparent and systemic approach to managing risks consistent with the risk appetite statement, maintaining liquidity and solvency and managing capital on an ongoing basis; and

(f) timely and to incorporate constructive feedback on risk exposure and risk management, to enable the Board and the senior management to take effective and informed decisions on risk appetite and capital management.

3.5 The policies and procedures which make up the ERM framework need to be properly documented and approved. Further, the following matters within the ERM framework should also be properly documented:

- the decision-making process;
- any management actions taken;
- any breaches occurred; and
- reviews and approvals made.

3.6 Where an authorized insurer is part of a group, the ERM framework should address the group risk in relation to other entities of the group (see section 6.5 for details). For this purpose, the process for identifying the group to which an authorized insurer belongs is set out in **Annex A**. In addition, where an authorized insurer has operations outside Hong Kong, any relevant risk needs to be managed adequately in a cross-border context.

[3] Please refer to paragraph 6.1.1 for the types of risks typically covered.

4. Governance

Objectives

An authorized insurer should maintain clear and well-documented risk management policies and procedures appropriate for the nature, scale and complexity of the risks associated with the business it conducts. These policies and procedures should describe the governance of risk management across the business, including roles and responsibilities, reporting lines and authority, as well as approaches, methodologies, process, controls, systems and reviews in relation to risk management activities.

The risk management policies and procedures should be approved by the Board. The Board may delegate the authority to the Risk Committee or senior management to approve operational procedures.

The ERM governance should be appropriate for the authorized insurer's Hong Kong operations and circumstances.

The Board

4.1 The Board has the overall responsibility to establish and oversee an effective ERM framework. In fulfilling the responsibility, the Board should give consideration and take actions to:

(a) establish an organizational structure for risk management, with clearly defined roles and responsibilities. This typically includes a Risk Committee, senior management and personnel responsible for risk management functions;

(b) ensure that the ERM framework is properly supported by suitable and sufficient resources;

(c) set up and embrace a sound risk culture [4] and effective risk management practices throughout the business;

[4] As reference, the Financial Stability Board issued the 'Guidance on Supervisory Interaction with Financial Institutions on Risk Culture' in 2014 <http://www.fsb.org/wp-content/uploads/140407.pdf > stated that '*A sound risk culture should emphasise throughout the institution the importance of ensuring that: (i) an appropriate risk-reward balance consistent with the institution's risk appetite is achieved when taking on risks; (ii) an effective system of controls commensurate with the scale and complexity of the financial institution is properly put in place; (iii) the quality of risk models, data accuracy, capability of available tools to accurately measure risks, and justifications for risk taking can be challenged, and (iv) all limit breaches, deviations from established policies, and operational incidents are thoroughly followed up with proportionate disciplinary actions when necessary'*.

(d) review at least annually and approve the risk appetite statement and ensure that it is effectively communicated and consistently adopted in the business activities;

(e) approve the risk management policies and key procedures;

(f) understand the risk exposure of the business and the approaches taken to control those risks;

(g) assess and approve material business activities that may deviate from the existing risk appetite and tolerable risk limits;

(h) critically review the results and assumptions underlying the ORSA, including, if any, the stress and scenario testing ("SST"), continuity analysis, business failure analysis and recovery plan;

(i) demonstrate the ongoing use of the ORSA's results as part of its strategic and other business decision-making process; and

(j) review the adequacy and effectiveness of the ERM framework, including the ORSA.

4.2 The Board may delegate[5] part of its authority in respect to the ERM to the Risk Committee or other competent individuals or committees. However, the Board shall retain ultimate responsibility. The Board needs to oversee the exercise of delegated authority by the relevant individuals or committees.[6]

4.3 The Board should articulate clearly the authority reserved to the Board in respect to the ERM and the manner in which the Risk Committee and senior management may report and escalate significant matters to them.

Risk Committee

4.4 As provided in the Guideline on the Corporate Governance of Authorized Insurers ("GL10"), all authorized insurers incorporated in Hong Kong as well as applicable overseas insurers (except for small

[5] Authorized insurers should refer to GL10 with regard to the expectation and guiding principles on delegations.

[6] For branches of overseas-incorporated insurers without a local Board in Hong Kong, the overseas Board may delegate the responsibility to the local functions i.e. the local Risk Committee and senior management as appropriate, but retains ultimate responsibility.

authorized insurers) are required to establish a Risk Committee.[7] All other authorized insurers are also encouraged to do so, and may consider establishing a local Risk Committee if the Risk Committee at group level does not take specific reference to the risk profile of the insurer.[8]

4.5 Where a Risk Committee is established, its ERM responsibilities would need to include the following matters, to the extent applicable:

(a) advising the Board on the authorized insurer's risk appetite as well as key risk management policies and procedures;

(b) independently reviewing the identification, measurement, monitoring and management of material risks and any areas of material non-compliance with the ERM framework;

(c) regularly reporting to the Board on matters of risk management and escalate issues of importance when necessary;

(d) advising the Board in risk quantification that may include appropriately challenging or validating risk and capital measures and models, stresses and scenarios used and its results; and

(e) advising the Board in reviewing the adequacy and effectiveness of the ERM framework.

4.6 In fulfilling its responsibilities, the Risk Committee should have full access to all necessary information provided by senior management and key person(s) in risk management functions.

Senior Management

4.7 Senior management has responsibilities for implementing the ERM framework and should endeavor to ensure that:

(a) day-to-day risk management activities are carried out in accordance with the approved risk policies and procedures of the ERM framework and in line with the risk appetite statement;

[7] Please refer to paragraphs 2.1(h) and 3.2 of GL10 for the definition of "small authorized insurers" and "applicable overseas insurers" respectively.

[8] In such case, the local Risk Committee may be in the form of a management committee and may not necessarily be a committee established at the Board level. However, the work of the local Risk Committee should be consistent to the overall objectives of the risk management governed by the Board.

(b) there is regular risk monitoring and risk reporting to the Board and/or Risk Committee and that material issues and material non-compliance with the ERM framework are quickly escalated to the Board and/or Risk Committee;

(c) adequate ERM training has been provided to the relevant staff on a regular basis; and

(d) appropriate communication channels are established such that relevant staff understand and adhere to the policies and procedures.

4.8 In carrying out its responsibilities, the senior management may delegate some of its responsibilities with respect to risk management to key persons in risk management function, with clear lines of accountability and reporting established and documented.

Risk Management Function

4.9 There should be a dedicated risk management function within an authorized insurer. The key person(s) in the risk management function has the responsibility to provide support and opinion to the Board, Risk Committee or senior management to establish and implement appropriate policies and procedures in relation to the ERM framework. This scope of responsibility would include providing support and opinion on the following matters in relation to the authorized insurer: solvency, capital and liquidity planning, product management, business planning, reinsurance and risk transfer strategy, ALM and investment strategies.

4.10 The IA expects an effective risk management function to have the following features:

(a) a direct reporting line to the Board and/or Risk Committee to ensure its independent assessment and prompt reporting of risks of the authorized insurer;

(b) be staffed by persons with the expertise and experience which are relevant and appropriate to the nature, scale and complexity of the authorized insurer's business operations;

(c) be objective and independent from the risk-taking and operational units the activities of which it reviews; and

(d) be timely in reporting identified risk management issues or other material matters that may have a significant impact on the authorized insurer's financial position and risk profile.

5. Risk Appetite Statement

Objectives

The Board should establish effective business strategies and make decisions that should be underpinned by a risk appetite statement appropriate to the nature, scale and complexity of the business operations.

The risk appetite statement of the authorized insurer should define the risk capacity and give clear guidance to operational management on the risk limits of material risks. Business planning and activities in business functions should align with the risk appetite statement.

5.1 The Board is ultimately responsible for, and to approve the risk appetite statement of the authorized insurer. An effective risk appetite statement would need to:

(a) be communicated across the business, and embedded in the business strategy and in day-to-day operations;

(b) comprise qualitative and quantitative measures that take into consideration relevant and material categories of risk and their interdependencies;

(c) take into account the authorized insurer's future business plan, and consider a range of plausible future scenarios; and

(d) be reviewed regularly or when there is a material change in the risks or business environment.

5.2 Actual or anticipated breaches of the established risk appetite statement or risk limits should be reported in a timely manner to the Risk Committee or senior management and, if necessary, escalated to the Board. The Board is expected only to approve activities that may significantly deviate from the risk appetite in rare cases and with good justification which should be documented.

6. Embedding the ERM Framework – Regular Risk Assessments and Control Process

Objectives

The authorized insurer should ensure that, as part of the ERM framework, risk assessments and control activities are performed regularly. The framework should be captured by appropriate risk management policies and procedures.

An authorized insurer should include the following regular risk assessment and control activities within its risk management policies and procedures:

(a) risk identification;
(b) risk quantification;
(c) risk monitoring and reporting; and
(d) risk management review and actions (e.g. mitigation or transfer)

The risk assessment and control activities should include a regular review of current and future risks against the insurer's risk appetite statement and risk limits structure.

6.1 Risk Identification

6.1.1 The ERM framework should require routine identification of all reasonably foreseeable and relevant material risks and risk interdependencies for risk and capital management as appropriate to the authorized insurer.

Where relevant and material, such risks (non-exhaustive) may include:

- insurance risk – including policy holder option risk;
- market risk – including spread risk;
- credit default risk;
- concentration risk – of assets and major reinsurer(s) (or retrocessionaire(s) for reinsurers);
- liquidity risk;
- operational risk;
- legal and compliance risks;
- conduct risk;
- cyber risk;
- reputational risk;

- strategic risk;
- political risk;
- emerging risks – e.g. climate risk; and
- group risk, for insurers being part of a group – including contagion risk.

6.1.2 The ERM framework should also consider the possibility that non-material risks could have a material impact on the authorized insurer when combined with other risks.

6.2 Risk Quantification

6.2.1 An authorized insurer should have policies and procedures on risk quantification. It should assess the level of risks to which it is exposed on a sufficiently regular basis, in terms of the potential impact and the probability of occurrence, using appropriate forward-looking techniques. Risk quantification may, to the extent it is necessary for the purposes of capturing the nature, scale and complexity of risks:

(a) encompass a sufficiently wide range of techniques, models and scenarios for effective risk and capital management (an example would be SST which is a common technique in assessing risks and the impact of potentially adverse movements in key risk factors);

(b) cover all material current and future risks, including risks not covered by the regulatory capital requirements; and

(c) be based on a consistent assessment of the authorized insurer's regulatory capital requirements and the Pillar 2 Capital amount (see paragraphs 6.2.3 to 6.2.5 for elaboration), taking into account the distribution of future cash flows to assess the level of risks.

6.2.2 An authorized insurer should give due consideration to appropriate management actions that may be taken in adverse circumstances to manage or mitigate its risks, and the timing of such management actions.

Relating Risk to Capital

6.2.3 Where the regulatory capital requirements does not adequately reflect the risks of the authorized insurer, a higher Pillar 2 Capital amount should be calculated for the purposes of this Guideline. The Pillar 2 Capital amount should reflect the full range of risks to which the

authorized insurer, including those that are not captured in the structure of the regulatory capital requirements calculation, or where the regulatory capital stresses do not adequately reflect the level of risk to which the insurer is exposed.

6.2.4 Subject to paragraph 6.2.3, an authorized insurer is generally expected to quantify its Pillar 2 Capital amount, and it should factor in the full range of risks to which the insurer is exposed, and assess whether the deviations from regulatory capital requirements are significant. The authorized insurer should document and explain in its ORSA Report its reasons for either adopting the regulatory capital requirements as its Pillar 2 Capital amount or a higher Pillar 2 Capital amount, particularly for specialty risks underwritten.

6.2.5 Where an authorized insurer assesses the Pillar 2 Capital amount for risk management purposes, the insurer should determine the target amount that it expects itself to hold at all times. This target amount should be commensurate with its stated business plans, risk appetite, risk mitigation initiatives, diversification and time horizon. For the avoidance of doubt, the actual level of capital held **must** be above the regulatory capital requirements at all times.

Use of Models in ERM

6.2.6 Where appropriate, authorized insurers may consider the need for suitable models to facilitate risk quantification and assessment of risk and capital adequacy. The outputs from the risk identification exercise should guide which material risks should be modeled, and inform any risk interdependencies.

6.2.7 Use of models in ERM does not necessarily refers to models used to determine capital requirements. For example, credit risk models can be used to monitor and manage credit risk as well as contribute to the determination of the Pillar 2 Capital amount.

6.2.8 Where a model is used in ERM, an authorized insurer should give consideration to the following factors:

(a) the complexity of the model, which should be commensurate with the nature, scale and complexity of risks taken;

(b) the expertise required in complex modelling activities;

(c) the basis for measuring risks in normal and severe adverse circumstances; and

(d) the regulatory capital requirements and Pillar 2 Capital amount associated with each material risk and the capital planning period.

6.2.9 The scope, usage and limitations of models and the associated risks of using model outputs should be well understood and acknowledged by all users of the models and model outputs, particularly the Board and senior management.

6.2.10 The risk and capital management models used should be consistently embedded in key business decision-making and risk management processes of the business. Key processes where models could be consistently embedded may include risk appetite monitoring, product development, investment, reinsurance, operational risk management, and key performance indicators for senior management.

6.2.11 To ensure the models meet the intended purpose and to minimize model risks, all models used as part of an authorized insurer's risk and capital management processes should be subject to regular review and ongoing validation such as back-testing. Independent review and validation is encouraged to ensure objectivity.[9]

Stress and Scenario Testing

6.2.12 An authorized insurer should conduct SST based on material risks to assess its risk profile and thus the relative movements in capital resources and capital requirements based on assumed adverse movements in key risk factors. SST involves considering an insurer-specific adverse event(s) and assessing its implications to the insurer.

6.2.13 Detailed considerations of SST[10] may include, to the extent applicable:

(a) the extent to which assumptions and adverse events in the SST are insurer-specific and relevant to the risk profile[11];

[9] For example, the personnel responsible for the review and validation of the model should be adequately qualified and should be independent of the personnel who design or own the model.

[10] Stresses and scenarios can be developed ranging from simple sensitivities to complex scenarios (deterministic or stochastic), with increasing sophistication and explanatory power. If necessary, an external party to the authorized insurer may be engaged to conduct the SST.

[11] Development of own scenarios could be referenced to pandemic scenario, catastrophic events leading to losses on multiple lines of business, sovereign default, counterparty default of most concentrated reinsurer (or retrocessionaire) or asset, severe economic recession, global financial crisis, mass policy holder surrenders, etc that are justified as relevant to the authorized insurer.

(b) sensitivity or stress analysis on a single risk factor or multi risk factors[12];

(c) the scope, identification and quantification of the relevant risk factors, e.g. risks factor dependencies or correlations, under both normal and stressed situations; and

(d) likely quantitative and qualitative impacts to the insurer within the modeled stresses and scenarios. In this regard, the modeled management actions required should be objective, realistic, achievable, adequate and legal.

6.2.14 An authorized insurer is expected to incorporate the results of the SST as inputs in business planning, risk decision making, solvency, liquidity and capital management, and in its ORSA.

6.2.15 The details (e.g. key assumptions and limitations in constructing the stresses and scenarios) and main outcomes of SSTs, together with the corresponding management actions are expected to be concisely presented in the ORSA Report (see paragraphs 9.4 to 9.5 for relevant details).

Continuity Analysis

6.2.16 Based on the nature, scale, and complexity of the business operations, an authorized insurer should consider conducting a regular forward-looking continuity analysis. The continuity analysis should analyze the ability of the insurer to continue in business, and the risk management and financial resources required to do so over a longer time horizon than that typically used to determine the regulatory capital requirements.

6.2.17 Continuity analysis may address the following matters specific to an authorized insurer, to the extent applicable:

(a) a combination of qualitative and quantitative elements in the medium and longer-term business strategy[13], projection of future financial

For non-quantifiable or operational risks such as legal, reputational, conduct, and cyber risks, an authorized insurer should consider assessment by scenario testing, taking into account the percentage probability of and the potential amount of losses.

[12] Sensitivity analysis could be used to assess the sensitivity of profits, capital resources and capital requirements to movements in, for example, lapses, claims, interest rates, etc either over a short or long period of time.

[13] The medium and longer-term business strategy would typically cover 3, 5 or more years.

position and analysis of the insurer's ability to meet the regulatory capital requirements on an on-going basis;

(b) planning for adverse scenarios and facilitating the development of management actions that deal with such situations; and

(c) development of contingency[14] or recovery plans (see considerations in paragraph 6.4.4) for use in going- and gone-concern situations to restore financial strength and viability.

Business Failure Analysis

6.2.18 Business failure is defined as the authorized insurer's solvency position falling below any regulatory capital requirements or the insurer being wound up for any other reason. Based on the nature, scale, and complexity of its operations, an authorized insurer should give consideration to perform analysis to identify scenarios that could result in business failure.

6.2.19 The use of reverse stress testing ("RST")[15] may be one of the means to conduct business failure analysis, with focus on identifying appropriate risk management actions. Alternative scenarios may cover operational dependency, reliance on parental financial support, limits to fungibility of capital, intra-group reinsurance, stock-lending or liquidity facilities.

6.3 Risk Monitoring and Reporting

6.3.1 The ERM framework should include risk management policies that set out how the results of the risk identification and risk quantification activities are monitored and reported to the Board, Risk Committee and senior management, together with clear reporting lines.

6.3.2 The monitoring and reporting activities should enable an authorized insurer, to the extent applicable, to:

(a) identify the sources and causes of risks;

[14] A contingency plan describes the necessary actions and resources to manage and control business disruption and losses. For example, a contingency plan may include plans designed to ensure that the essential business functions could continue to operate during and after a disaster.

[15] Depending on the nature, size and complexity of the insurer and risks it faces, RST could be performed through quantitative modelling, qualitative analysis, or hybrid approach. RST could start with the outcome of a business failure or the financial condition falling below a predefined level, and then analyzing different scenarios under which such failure or financial condition may occur.

(b) present the results of risk identification and risk quantification activities, as well as evaluating the level and trend of material risks;

(c) perform the activities sufficiently frequently and in a timely way to ensure that management can take swift actions to address areas of concern;

(d) compare the results against the risk appetite statement and risk limits structure, highlighting material areas of actual or potential, current or future breaches;

(e) raise awareness of matters that have or are likely to have a materially adverse effect on the solvency, reserve, liquidity or financial condition of the insurer;

(f) conduct the activities in a clear and concise manner yet comprehensive enough to facilitate informed decision-making; and

(g) include the results above into the ORSA Report (see section 9 for detailed requirements).

6.3.3 Risk monitoring and reporting should cover relevant material risks and the depth and scope of the reporting should be consistent with the nature, scale, and complexity of the authorized insurer's operations, risk profile and risk appetite.

6.3.4 To ensure the data integrity of the risk reports, an authorized insurer should maintain processes to validate, test, aggregate and reconcile data and regularly assess the degree to which data is error free.

6.3.5 The Board and senior management should periodically review that the information, in terms of both amount and quality, and the extent to which it remains relevant and appropriate to risk governance, risk management process and risk appetite, and to the decision-making processes. An authorized insurer is expected to take effective and timely remedial actions to address deficiencies in risk reporting practices.

6.4 Risk Management Review and Actions

6.4.1 The ERM framework should enable well-informed business decisions and risk management actions to be taken. The identification and

quantification of risks should ensure appropriate and timely management actions are taken when required.

6.4.2 The authorized insurer should document its risk management policies towards risk retention and reinsurance or risk transfer strategies, e.g. use of derivatives, diversification or specialization, ALM, treatment of any off-balance sheet items and non-traditional forms of reinsurance, etc.

6.4.3 An authorized insurer must take every practicable step to safeguard its assets and ensure that the value of its assets is not less than the aggregate of the amount of its liabilities and the applicable level of solvency under the Ordinance. Besides, the authorized insurer should maintain a buffer above the statutory solvency margin at all times for prudent risk and capital management purposes.

6.4.4 Based on the nature, scale, and complexity of the operations, an authorized insurer should maintain a recovery plan for planning and managing severe adverse situations, which should also be included in the ORSA. The recovery plan should address the following matters specific to the authorized insurer, to the extent applicable:

(a) the relevant entities and their interconnectedness;

(b) identification of functions or services significant to continuation;

(c) a pre-defined quantitative and qualitative trigger framework[16] in which recovery options are triggered in the face of a range of severe adverse situations;

(d) an assessment on the timeliness and creditability of the recovery options[17] in both going and gone concern situations;

(e) measures to restore financial viability e.g. recapitalization and capital conservation that may take into account intra-group transactions;

(f) strategies for communication with stakeholders; and

[16] Possible triggers based on liquidity, market conditions, macro-economic conditions, and operational conditions.

[17] Typical recovery options may include, for example, capital raisings, disposal of business units, transitioning business to run-off or increasing the overall level of reinsurance. Recovery options may be assessed from the perspective of speed and timing, operational aspects of execution, impediments, risks and necessary preparation required.

(g) periodic review of the recovery plan and options.

6.4.5 Management actions identified in ERM should be objective, realistic, achievable, adequate and legal. There should be a proper approval process on the management actions at Board level or senior management level, where appropriate.

6.5 Requirements in ERM Processes in respect of Group Risk

6.5.1 The ERM framework of an authorized insurer that belongs to a group should meet the following minimum requirements in respect of managing group risk.

6.5.2 The Board and senior management of an authorized insurer should set risk management policies in respect of group risk of the insurer.

6.5.3 The ERM framework of the authorized insurer should enable its Board and senior management to understand the risks associated with the intra-group transactions, as well as the inter-relationships and interdependence among group entities, that have a material impact on the insurer.

6.5.4 The Board and senior management of the authorized insurer should have a clear understanding of the reinsurance activities conducted at the group level relevant to the authorized insurer. They should consider possible knock-on effects impacting the solvency and liquidity positions of the authorized insurer, that are arising from any failure of these reinsurers would have.

6.5.5 The ERM framework of the authorized insurer should give consideration to the risk of support to the insurer from group entities not being available when there is a concern about another part of the group. In some circumstances, this may entail monitoring, setting quantitative and qualitative restrictions and reporting significant group events and intra-group exposures that materially impact the insurer, as appropriate.

7. Embedding the ERM Framework – Business Activities

Objectives

An effective ERM framework should include explicit risk management policies setting out the risk management approach in relation to material risks. These policies should be commensurate to the authorized insurer's business strategy, risk appetite statement, capital management and ORSA.

Risk management policies should be proportionate to the nature, scale and complexity of the business operations.

7.1 The Board should ensure that the ERM framework is embedded in business activities.[18] This should include developing and maintaining risk management policies in business areas where risk is actively taken or transferred, including where relevant and material:

- underwriting (section 7.4)
- asset liability management (section 7.5)
- investment (section 7.6)
- reinsurance and risk transfer (section 7.7)
- liquidity (section 7.8)

7.2 As part of the embedding of the ERM framework into its business activities, the authorized insurer should also develop and maintain other risk management policies, including where relevant and material, the following policies:

- actuarial policy (section 7.9)
- conduct risk policy (section 7.10)
- cyber risk policy (section 7.11)
- claims management policy (section 7.12)
- internal controls policy (section 7.13)
- data quality policy (section 7.14)

7.3 The risk management policies listed in paragraphs 7.1 and 7.2 and the corresponding guidance in paragraphs 7.4 to 7.14 are neither exhaustive nor mandatory. Authorized insurers have the flexibility to design their ERM framework to accord with their own specific circumstances.

[18] In the case of the product life-cycle, this would involve multiple activities and policies.

Risk Management Policies Where Risk Is Actively Underwritten or Transferred

7.4 ***Underwriting***

7.4.1 The ERM framework should include a prudent risk management policy on underwriting (or underwriting policy), as appropriate, that clearly specifies the nature, role and extent of underwriting activities[19].

7.4.2 The underwriting policy should address the approaches and controls which the authorized insurer has in place for the following matters:

(a) the nature and amount of risk the insurer underwrites and linkages to the risk appetite statement;

(b) the identification of underwriting risks including, preferably, emerging risks;

(c) the quantification of underwriting risk, including its quantification for the purposes of factoring it into the calculation of the regulatory capital requirements and its Pillar 2 Capital amount;

(d) monitoring and reporting of underwriting risks;

(e) mitigation and control of underwriting risks;

(f) the transfer of underwriting risks and interaction with the reinsurance and risk transfer policy and associated credit risk; and

(g) regular review of underwriting activities and the underwriting policy.

7.4.3 The underwriting policy should ensure that the impact on regulatory capital requirements and the Pillar 2 Capital amount are considered whenever there is an anticipated material change in the underwriting risks accepted by the authorized insurer.

7.4.4 An authorized insurer should adopt a prudent underwriting policy and should not underwrite any risk beyond its financial capacity or insurance expertise. Where appropriate, independent professional valuation or advice should be sought for the purpose of assessing risk in the underwriting process.

[19] Underwriting activities may include pricing, claims settlement and expense control (where applicable and relevant to the expenses of the underwriting activities).

7.5 *Asset-Liability Management*

7.5.1 The ERM framework should include a risk management policy on ALM (or ALM policy), as appropriate, that clearly specifies the nature, role and extent of ALM activities and their relationship with product development, pricing functions and investment management.

7.5.2 The ALM policy should address the approaches and controls which the authorized insurer has in place for the following matters:

(a) the application of the risk appetite statement and the risk limits structure to the insurer's willingness and capacity to bear ALM risks;

(b) the identification of ALM risks, taking into account any off-balance sheet exposures and associated contingent risks; legal restrictions to assets or liabilities; and interdependencies with other risks, including cross-border, legal and other non-quantitative risks;

(c) the quantification of ALM risks under an appropriate range of plausible and adverse scenarios;

(d) the management of ALM risks, including where appropriate:

- how investment and liability strategies allow for the interaction between financial assets and technical provisions;
- how the liability cash outflows will be met by the cash inflows under different economic conditions;
- how ALM strategies may apply to different or homogeneous blocks of assets and liabilities;
- how ALM strategies are considered with regulatory capital requirements and the Pillar 2 capital amount;
- how duration, currency, interest rate and other mismatches are managed, particularly for long duration insurance liabilities exposing an insurer to reinvestment risk; and
- how guarantees and embedded options within insurance policies are matched;

(e) monitoring and reporting of ALM risks; and

(f) regular review of ALM activities and the ALM policy.

7.6 *Investment*

7.6.1 The ERM framework should include a risk management policy on investment (or investment policy), as appropriate, that specifies the nature, role and extent of its investment activities.[20]

7.6.2 The investment policy of an authorized insurer should identify appropriate controls which the insurer has in place for the following matters:

(a) the insurer's capacity to bear investment risk is appropriate for and in line with its risk appetite statement and risk limits structure, types of business, capital and liquidity needs;

(b) the identification of risks arising from investment activities, particularly for assets that are less transparent or subject to less governance or regulation;

(c) the competency of staff and of any external investment providers involved in the investment processes, so that they fully understand the insurer's investment objectives and adhere to the investment policy and strategies;

(d) sufficient management of counterparty credit and concentration risks;

(e) the safe-keeping of assets and accurate recording of investment activities;

(f) timely actions to identify any significant investment losses and to make provision for them;

(g) the manner in which investment strategies and allocation are factored into regulatory capital requirements and the Pillar 2 Capital amount;

(h) the close monitoring of any engagements of investment tools such as derivatives;

(i) the minimization of legal and basis risks; and

(j) regular reviews of the investment performance, investment strategy and investment policy.

[20] Authorized insurers are required to observe the Guideline on Asset Management by Authorized Insurers ("GL13")

7.6.3 The Board has the core responsibility for the formulation and implementation of the investment policy. In particular, due attention must be given to ensure any complicated investment strategy, sophisticated financial instruments and use of derivatives, if any, remains commensurate with business needs.

7.6.4 Policy holder funds should be prudently managed. Where appropriate, and without limitation, there should be procedures which address the following matters:

(a) the prudent management of funds for authorized business under the Ordinance or other regulations; and

(b) the maintenance of a separate set of books and accounts for policy holder funds.

7.7 *Reinsurance and Risk Transfer*

7.7.1 The ERM framework should include a risk management policy on reinsurance and risk transfer (or reinsurance and risk transfer policy), as appropriate, that ensures adequate and appropriate reinsurance arrangements for the risks underwritten, reflecting the insurer's risk profile, business strategy and risk appetite. [21]

7.7.2 The reinsurance and risk transfer policy of an authorized insurer should address the approaches and controls which the insurer has in place for the following matters:

(a) the adequacy and suitability of reinsurance arrangements for the risks underwritten and the impact on the insurer's capital requirements and liquidity management;

(b) the creditworthiness and the security of the participating (re)insurers, including reinsurance recoverable and intra-group reinsurance arrangements, and periodically review of the collectability of the amounts due from them;

(c) the appropriate use of any non-traditional forms of reinsurance or risk transfer to capital markets or special purpose entities and use of derivatives;

[21] Authorized insurers are also required to observe the Guideline on Reinsurance with Related Companies ("GL12") and the Guideline on Reinsurance ("GL17") issued by the IA.

(d) the assessment of cross-border reinsurance or risk transfer;

(e) how reinsurance and risk transfer strategies are factored into the insurer's regulatory capital requirements and the Pillar 2 Capital amount;

(f) the assessment on the effectiveness of reinsurance or risk transfer arrangements under adverse financial conditions;

(g) monitoring and reporting of reinsurance or risk transfer risks; and

(h) regular review of the reinsurance and risk transfer policy.

7.8 *Liquidity*

7.8.1 The ERM framework should include a risk management policy on liquidity (or liquidity policy), as appropriate, to ensure liquidity adequacy across time horizons under current and plausible stress scenarios.

7.8.2 Liquidity risk is concerned with both assets and liabilities as well as their interplay. Liquidity risk is the uncertainty, emanating from business operations, investments, reinsurance arrangements or financing activities, over whether the authorized insurer will have the ability to meet payment obligations in a full and timely manner in current or stressed environments.[22]

7.8.3 The liquidity policy of an authorized insurer should address the approaches and controls which the insurer has in place for following matters:

(a) the identification of liquidity sources and of liquidity needs across various time horizons and under current and plausible stress scenarios;

(b) the setting of quantitative targets for liquidity risk;

(c) monitoring and reporting of liquidity risk; and

(d) regular review of liquidity management and planning as well as the liquidity risk policy.

[22] For example, a policyholder run may expose the authorized insurer to a substantial level of liquidity risk.

Other Risk Management Policies

7.9 *Actuarial*

7.9.1 The ERM framework should include a risk management policy on actuarial matters (or actuarial policy), as appropriate, that ensures the appropriateness of the data, methodologies and underlying models and assumptions used. As guidance, an actuarial function[23] should be capable of evaluating and providing advice regarding matters on, for example, technical provisions, premium and pricing activities, capital adequacy, reinsurance and compliance with related statutory and regulatory requirements.

7.9.2 The actuarial policy should address the approaches and controls which the authorized insurer has in place for the following matters:

(a) the methodologies, models and assumptions used in calculations of the solvency position, regulatory capital requirements, technical provisions, premium and pricing;

(b) capital adequacy assessments and stress tests under various scenarios, and their impact on assets, liabilities, and actual and future capital levels;

(c) development, pricing and assessment of the adequacy of the reinsurance arrangements;

(d) distribution of bonuses or dividends for participating policies, if applicable;

(e) risk modelling in the ORSA;

(f) the setting of materiality thresholds or risk limits to facilitate monitoring and reporting of actuarial-related risks[24]; and

(g) regular review of actuarial-related risk management arrangements.

7.9.3 The methodologies, models, and assumptions should take into account the business volume, actual claims experience of the authorized insurer, industry practice, types of insurance product and

[23] This does not restrict the carrying out of the actuarial function by several divisions or departments within an authorized insurer.

[24] Actuarial-related risks cover risks evaluated and monitored by the actuarial function according to its ERM framework and the ORSA.

the trend of court awards or other applicable considerations. As such, it is essential for the authorized insurer to build up a database that consists of the historical claims data; and an actuarial system that determines the liabilities of insurance business and ensures a prudent and satisfactory relationship between the nature and term of the assets and the nature and term of its liabilities, if applicable**.**

7.9.4 Any reserving assumptions made should be periodically reviewed to ensure that due recognition has been given to changes in the composition of the business portfolio, market and legislative developments, etc.

7.9.5 An authorized insurer that carries on employees' compensation and/or motor insurance businesses is also required to observe the Guideline on Actuarial Review of Insurance Liabilities in respect of Employees' Compensation and Motor Insurance Businesses ("GL9") and arrange for the reserves of those classes of business to be subject to actuarial review as appropriate.

7.10 ***Conduct***

7.10.1 The ERM framework should include a risk management policy on conduct risk (or conduct risk policy), as appropriate, that ensures fair treatment of customers.[25] Sources of conduct risks are inherent in the nature of insurance business and service provision. An authorized insurer has the responsibility for good conduct of business throughout the insurance life-cycle, and for extending good conducts to those functions or activities that are outsourced.

7.10.2 The conduct risk policy should reflect processes and procedures to identify, monitor, manage or mitigate conduct risk in the provision of insurance products and services to policy holders and customers.

7.10.3 Conduct risk identification may be relatively qualitative. The conduct risk policy of an authorized insurer should address the approaches and controls which the insurer has in place for the following matters:

(a) dealing with potential policy holders and existing policy holders with due skill, care and diligence;

(b) conducting business taking into account the customers' and the policy

[25] An authorized insurer is required to observe relevant Guidelines and Codes issued by the IA and Codes of Conduct and Codes of Practice issued by industry bodies, where applicable.

holders' reasonable expectations;

(c) using all reasonable endeavours to conduct business in a way that enables policy holders to make informed decisions regarding any contracts of insurance offered by the insurer;

(d) the product design and development, marketing, disclosures and distribution of insurance products and sales incentives, and reasonable expectations of its target market;

(e) timely communication to customers on policy information and the integrity of policy advice;

(f) maintaining good quality of policy servicing, including claims handling, and complaints handling;

(g) resolving conflict of interests supported by appropriate governance and control mechanisms;

(h) establishment of indicators to enable monitoring and reporting of conduct risk; and

(i) performing a regular review of the conduct risk management arrangements and policy.

7.10.4 Implementation of the conduct risk processes and procedures dealing with fair treatment of customers should be effectively monitored and timely evaluated. Deficiencies identified should be properly remedied.

7.11 *Cyber*

7.11.1 The ERM framework should include a risk management policy on cyber risk (or cyber risk policy), as appropriate, that is commensurate with the scale and complexity of the business, to identify, prevent, detect and mitigate cyber security threats.[26]

7.11.2 The cyber risk policy of an authorized insurer should address the approaches and controls which the insurer has in place for the following matters:

(a) protection of the personal data of its policy holders, and digital or

[26] Authorized insurers are also required to observe the Guideline on Cybersecurity issued by the IA.

electronic data of its business to ensure continuity of its business operations;

(b) identification, prevention, detection and mitigation of cyber security threats;

(c) identification of cyber security threats arising from technology tools and platform such as computer systems, mobile applications, the internet and telecommunication networks;

(d) periodic testing on the robustness of the mitigation measures to deal with the cyber security threats timely and effectively;

(e) approach and frequency on monitoring and reporting of cyber risks, including to other law enforcement authorities where applicable; and

(f) regular review and assessment on the cyber security policies and procedures, as well as monitoring of their implementation.

7.11.3 An authorized insurer should also communicate the relevant policies and procedures to its staff and as appropriate to other users of the cyber security system concerned.

7.12 *Claims Management*

7.12.1 The ERM framework should include a risk management policy on claims management (or claims management policy), as appropriate, for the settlement of claims and to ensure that any claims reported are promptly recorded and the relevant and adequate reserves are provided for accordingly.

7.12.2 The amounts of estimated and actual claims should be compared from time to time to ensure that adequate provisions are made for outstanding claims. There should be escalating procedures to notify the Board and senior management of large or fraudulent claims, particularly those that are likely to materially impact the authorized insurer's regulatory capital and Pillar 2 Capital amount positions.

7.13 *Internal Controls*

7.13.1 The ERM framework should include internal controls, systems and functions[27] (or internal controls policy) that are adequate for the authorized insurer's objectives, strategies, risk profile, and the applicable legal and regulatory requirements, and be adaptable to internal and external changes.

7.13.2 The internal controls policy should address the controls, systems and functions which the authorized insurer has in place for the following matters:

(a) the need for appropriate segregation of duties and prevention of conflicts of interest;

(b) the incorporation of appropriate internal controls relevant to the key activities, critical information technology ("IT") functionalities, access to critical IT infrastructure by staff and related third parties, and important legal and regulatory obligations of the authorized insurer;

(c) the inclusion of procedures to identify potential suspicious transactions[28];

(d) the inclusion of information processes to obtain internal financial, operational and compliance data, as well as external market information relevant to decision making;

(e) approach and frequency on monitoring and reporting of internal control risk and events; and

(f) regular review of internal controls, systems and activities to assess that they are adequate and adaptable to internal and external changes.

7.13.3 Adequate communication and training should be in place to ensure all staff fully understand and adhere to the internal controls and their respective duties and responsibilities as well as reporting lines.

[27] 'Control, systems and functions' here includes the strategies, policies, processes and controls in place. This does not restrict the carrying out of the functions related to internal controls by several divisions or departments within an authorized insurer.

[28] This is **not** restricted to authorized insurers that carry on long term business which are required to observe the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("GL3"), for preventing and identifying any suspicious money laundering activities.

7.13.4 Separation of critical functions, cross-checking of documents, dual control of assets and double signatures on certain documents, etc., are the types of controls which the authorized insurer should consider implementing to ensure appropriate checks and balances are in place, together with clear and well defined reporting lines.

7.14 *Data Quality*

7.14.1 The ERM framework should include a risk management policy on data quality (or data quality policy), as appropriate, that ensures data, (both internally developed and externally supplied) is current, accurate and complete; and protects an authorized insurer against the risk of loss from inadequate or failed internal processes, people and systems or from external events impacting data quality.

7.14.2 The data quality policy should address the approaches and controls which the authorized insurer has in place for the following matters:

(a) the use of sufficient, reliable and relevant data for the insurer's key processes, such as underwriting, pricing, reserving and reinsurance;

(b) safeguards against operational risk events such as theft of data, breach of regulations, disclosure of sensitive data or business disruption arising from data corruption;

(c) accuracy and reliability of data aggregation;

(d) approach and frequency on monitoring and reporting of data quality deficiencies; and

(e) regular review of data quality controls, systems, and policy.

7.14.3 An authorized insurer should have appropriate measures or plans in place to address deficiencies in its risk data aggregation capabilities and rectify poor data quality in a timely manner.

8. ERM Framework Review

Objectives

The ERM framework and the ORSA should be responsive to changes in the risk environment and risk profile to enable continual improvement in the effectiveness of risk management.

The ERM framework should be reviewed to ascertain that the ERM framework remains fit for purpose and the review results should be incorporated in the ORSA Report.

8.1 Changes in the risk environment or risk profile could come from:

- material transactions;
- internal or external events;
- changing expectations of policy holders and shareholders; or
- emerging or new risks, etc.

8.2 Depending on the nature, scale and complexity of an authorized insurer, the effectiveness of the ERM framework and the ORSA should be regularly reviewed in order to ascertain that the ERM framework remains fit for purpose. There should be a feedback loop to make necessary and timely remedial actions or improvements to the ERM framework and the ORSA.

8.2.1 The effectiveness of the ORSA should be regularly validated through independent review [29] by suitably experienced individual(s) who report directly to, or are themselves members of the Board.

8.3 Risk reporting should be reviewed on a regular basis to ensure it remains relevant and appropriate, in terms of both extent and quality of information, to the risk governance and decision-making process.

8.4 Specifically, SSTs should be updated in light of new risks, better understanding of risk exposures of business, new techniques or models, and updated data sources.

8.4.1 Validation of SSTs should be conducted on a reasonably frequent basis. The validation may, as appropriate, include the underlying assumptions of the SSTs, the sufficiency of the severity of the SSTs,

[29] Independent review may be carried out by an internal or external body as long as the reviewer is independent, is not responsible for, and has not been actively involved in, the part of the ERM framework that it reviews.

the robustness of the data applied in SST calculations, the performance of adopted technique or models, and the reasonableness of the results.

8.4.2 Corrective actions should be undertaken if material deficiencies are identified or if SSTs are not adequately taken into consideration in the overall business decision-making process.

9. Own Risk and Solvency Assessment (ORSA)

Objectives

As part of the regular cycle of risk assessment, an authorized insurer should regularly perform an ORSA to assess its risk profile, the adequacy of its risk management and also its current, and likely future, solvency and liquidity positions.

The ORSA should enable an authorized insurer to:

(a) determine the overall financial resources it needs to manage its business given its risk appetite and business plans;

(b) assess the quality and adequacy of capital resources to meet regulatory capital requirements and any additional capital needs, including recapitalization; and

(c) be forward-looking with a time horizon consistent with business planning, and remain viable under both normal and stressed conditions.

9.1 All authorized insurers which are subject to this Guideline are required to conduct an ORSA. The IA expects the main outcomes of the ORSA in the form of a report ("ORSA Report") that considers the minimum requirements in paragraphs 9.4 and 9.5.

9.1.1 Notwithstanding the mode of operation of the authorized insurer in Hong Kong, i.e. either as a Hong Kong incorporated company or as a Hong Kong branch of an overseas incorporated company, the ORSA Report submitted to the IA should cover the entire company with separate specifics to cover the Hong Kong operations.

9.1.2 In relation to paragraph 9.1.1, a Hong Kong branch of an overseas incorporated may submit either (i) a combined ORSA Report for the entire company with separate specifics of Hong Kong operations; or (ii) separate sets of ORSA Reports – one for the entire company and one for the Hong Kong branch. In both cases, only the part of the ORSA Report in relation to the Hong Kong branch is required to meet the minimum requirements of the ORSA under this Guideline.

9.2 An authorized insurer should also consider its exposure to group risk and perform its ORSA at a level consistent with the way its operations and material risks are managed.

9.3 The Board and senior management are accountable for the content of the ORSA. The ORSA should be performed at least annually, and whenever there are material changes to the risk profile of the authorized insurer, so that the ORSA continues to provide relevant information for decision making at the Board, Risk Committee and senior management levels and for the purposes of the risk management control functions.

Minimum Requirements of ORSA Report

9.4 An ORSA Report should cover the following matters in a concise manner:

(a) all material activities of the regular cycle of risk assessment (see sections 5, 6 and 7 for details) that includes an analysis of key drivers of the change in the financial and capital adequacy positions, summary of methodologies, models and assumptions to determine the regulatory capital requirements and the Pillar 2 Capital amount; and

(b) a review of the effectiveness of the ERM framework (see section 8 for details).

9.5 The ORSA undertaken by an authorized insurer should be appropriate to the nature, scale and complexity of its risks. It should include, without limitation, the following matters:

(a) the risk appetite statement;

(b) the description of the ERM framework and the year-on-year key changes;

(c) an assessment of the effectiveness of the ERM framework;

(d) an analysis of the business strategy evidenced by significant or unusual growth or shifts in business volumes, new lines of business or operations;

(e) the considerations for each foreseeable and relevant material risk, explicitly stating which risks are quantifiable and which are not quantifiable;

(f) a description of the measures or criteria used to identify and assess risks, the risk limits structure, and the Pillar 2 Capital amount needed to meet those risks;

(g) a summary of the quantitative and/or qualitative risk assessments in both normal and adverse situations for each material risk, including, if any, risk arising from non-insurance entities (regulated or unregulated) and partly-owned entities controlled by the insurer;

(h) the assessments of the regulatory capital requirements and the Pillar 2 Capital amount given the risk appetite, business plans and the risk management actions;

(i) reasons attributed to differences between the actual and planned, regulatory capital requirements and the Pillar 2 Capital amount outcomes;

(j) any breaches of risk limits with causes and remediation actions taken and the further actions taken to prevent future breach;

(k) the SST results, including the impact on the regulatory capital requirements and the Pillar 2 Capital amount, on both the IA prescribed scenarios and the insurer's own scenarios with details of management actions and their impact with explanation and justification. In reporting to the IA, the prescribed scenarios:

(i) For long term insurance business, authorized insurers should include the scenarios provided in the Actuarial Guidance Note 7 on Dynamic Solvency Testing ("AGN7") issued by the Actuarial Society of Hong Kong[30]; and

(ii) For general insurance business, authorized insurers should include the scenarios as prescribed by the IA from time to time;

(l) an analysis of the quality and adequacy of financial resources under normal and adverse scenarios;

(m) if any, the conclusions from continuity analysis and business failure analysis on the ability to meet the regulatory capital requirements on an on-going basis and to remain solvent;

[30] The scenarios are in accordance with AGN7 until further notice.

(n) if any, the recovery plan and the assessments of the recovery options; and

(o) if any, an analysis of activities, products and other exposures that expose the authorized insurer to systemic risk that may materialize to have a wider impact that extends from the insurance sector to the financial markets.

10. Reporting to the Insurance Authority and Supervisory Review

10.1 All authorized insurers which are subject to this Guideline are required to prepare their ORSA Report as at each financial year-end date annually or as at a date when there are material changes in the risk profile, and submit the ORSA Report to the IA within four months of the relevant date.

10.2 The IA requires approval of the ORSA Report at the Board or Risk Committee level. Deliberations on the ORSA's main outcomes should be minuted for supervisory review.

10.3 An authorized insurer that belongs to a group may make use of its group's ORSA report, provided that the required details specific to the Hong Kong operations are clearly and concisely documented in the ORSA Report and comply with the requirements of this Guideline.

10.4 Subject to paragraphs 10.1 to 10.3, where two or more authorized insurers belong to the same group, these insurers may apply in writing to the IA for an approval to submit a single combined ORSA Report instead of multiple ORSA Reports. When deciding whether or not to approve such application, the IA would take into account the extent to which the local management structure, risk governance and the ERM framework of the authorized insurers making the application, are shared.

10.5 An authorized insurer that is part of a group, if permitted by applicable law, regulations and rules, is required to provide written prior notification to the IA of group events and intra-group transactions that are material to the insurer's operations in Hong Kong together with the expected impact of the events or transactions. Examples of notifiable intra-group transactions or events are set out in **Annex B**.

10.6 This prior notification procedure referenced in paragraph 10.5 is not an approval process. Rather it serves to facilitate the IA's monitoring of the authorized insurer's group risks, its interactions and dealings with other group entities and any potential impact on the solvency, liquidity and profitability of the insurer.

10.7 ***Supervisory Review and Expectations***

10.7.1 In reviewing the ERM framework, including the ORSA Report, the IA would give due regard to the operational scale and complexity of the authorized insurer. The IA's approach in this respect is one of

"substance over form". Authorized insurers may need to explain the deviations from or alternatives to the guidance and minimum requirements outlined in this Guideline. The IA would carefully consider and evaluate the explanations.

10.7.2 Where necessary to safeguard the interests of policy holders, the IA would require an authorized insurer to:

(a) strengthen the ERM framework, solvency and liquidity assessments and capital management processes;

(b) demonstrate the capability of models used, including the basic operations, important relationships, major sensitivities, strengths and potential weaknesses;

(c) demonstrate that the Board has based its business decisions or risk management approach on considerations of regulatory capital requirements and Pillar 2 Capital amount, financial resources, and its ORSA on an ongoing basis;

(d) demonstrate that risk management actions in the ORSA have been properly and effectively undertaken;

(e) arrange for an independent party to review the effectiveness of the ERM framework; and

(f) undertake appropriate actions or plans to strengthen policy holders' protection.

11. Implementation

11.1 This Guideline shall take effect from 1 January 2020. Subject to paragraph 11.2, an authorized insurer should submit its first ORSA Report to the IA for its financial year ending on or after 31 December 2020.

11.2 The IA is in the process of developing the regulatory capital requirements under Pillar 1 of the RBC regime ("Pillar 1 RBC Requirements"). The period between a) 1 January 2020 and b) the date on which the Pillar 1 RBC Requirements come into force and become applicable to authorized insurers, shall be referred to as the Initial Period, for the purposes of this paragraph 11.2 and paragraph 11.3. During the Initial Period, an authorized insurer may (in place of paragraph 10.1):

(a) submit its ORSA Report using a valuation date other than its financial year-end date, but in no event more than three months earlier than the financial year-end date; and/or

(b) submit its ORSA Report within six months of the valuation date.

11.3 Solely for the purpose of preparing the ORSA Report during the Initial Period, instead of using the regulatory capital requirements calculated per the requirements in the Ordinance for inclusion in the ORSA Report, an authorized insurer shall instead use the prescribed capital requirements that were calculated in its response to the most recent Quantitative Impact Study ("QIS Capital Requirements") prior to the valuation date of its ORSA Report and all references to "regulatory capital requirements" as it applies to the ORSA Report in this Guideline shall be deemed as references to the QIS Capital Requirements for ORSA Reports submitted during the Initial Period.

[Month] 2019

Glossary

Basis risk	The risk that the relationship between two financial variables will change, particularly between two sorts of interest rate or generally between a hedge and the hedged position.
Capital adequacy*	The adequacy of capital resources relative to the regulatory capital requirements.
Capital resources*	Financial resources that are capable of absorbing losses.
Conduct risk**	As part of operational risk, the risk (or conduct of business risk) that can be described as the risk to customers, insurers, the insurance sector or the insurance market of financial loss or other adverse consequences that arises from insurers and/or intermediaries conducting their business in a way that does not ensure fair treatment of customers or results in harm to customers. This description includes the risks to which insurers, intermediaries and the insurance sector may be exposed as a result of their poor business conduct, as well as the risks to which such conduct exposes their customers.
Group risk*	The risk that the financial condition or continued operation of the authorized insurer may be adversely affected by an event that is either internal or external to the group it belongs. Such an event may either be financial or non-financial.
Key person(s) in risk management / actuarial control functions	The individual(s) approved by the IA under section 13AE of the Ordinance and responsible for the performance of the risk management or actuarial control functions, as the case may be, of an authorized insurer.
Legal risk*	The risk that an insurer may be adversely affected due to legal uncertainty that can arise from unenforceable contracts, change in laws or regulations, or failure to properly comply with laws or regulations.
Model risk	The risk of adverse consequences (e.g. financial loss, poor decision making, or damage to reputation) arising from the

	improper design, development, implementation and/or use of a model. This risk can originate from, among other things, incorrect parameter estimates; flawed hypotheses and/or assumptions; inaccurate, inappropriate or incomplete data; and inadequate monitoring and/or controls.
Operational risk*	The risk arising from inadequate or failed internal processes or systems, behaviour of personnel or from external events. Operational risk includes legal risk and the portion of conduct risk that impacts insurers, but excludes strategic and reputational risk.
Pillar 2 Capital amount	The amount that reflects all material risks of the authorized insurer, including those which are not captured in the structure of the regulatory capital requirements calculation, or where the regulatory capital stresses do not adequately reflect the level of risk to which the insurer is exposed. Pillar 2 Capital amount may be equal to or higher than the regulatory capital requirements.
Political risk*	The risk an insurer faces because of political changes or instability in a jurisdiction, country or region.
Regulatory capital requirements	Mean the set of solvency and capital requirements as prescribed or specified in the Ordinance.
Reputational risk*	The risk that potential negative publicity regarding an authorized insurer's business practices, whether true or not, will cause a decline in the customer base or brand value of the insurer, costly litigation, or revenue reductions.
Reverse stress testing*	Identifies scenarios that are most likely to cause an authorized insurer to fail, and focuses on appropriate risk management actions.
Risk appetite*	The aggregate level and types of risk an authorized insurer is willing to assume within its risk capacity to achieve its strategic objectives and business plan.
Risk capacity*	The maximum level of risk an authorized insurer can assume given its current level of resources taking into account of its regulatory capital requirements, Pillar 2

	Capital amount, liquidity needs, the operational environment (e.g. technical infrastructure, risk management capabilities, expertise) and obligations to policy holders, shareholders and other stakeholders.
Risk limit*	Quantitative measure based on an authorized insurer's risk appetite which gives clear guidance on the level of risk to which the insurer is prepared to be exposed and is set and applied in aggregate or individual units such as risk categories or business lines.
Risk limits structure*	The aggregate set of risk limits which the authorized insurer imposes on its material risks and their interdependencies, as part of its ERM framework.
Risk profile*	Point in time assessment of the authorized insurer's gross and, as appropriate, net risk exposures aggregated within and across each relevant risk category based on forward-looking assumptions.
Scenario testing*	Testing which considers the impact of a combination of circumstances to reflect extreme historical or other scenarios which are then analyzed in light of current conditions. Scenario testing may be conducted deterministically or stochastically.
Senior management	Refers to the set of individuals reporting to the chief executive and is responsible for managing the business of an authorized insurer on a day-to-day basis and/or performing a function that is likely to have a significant influence on the business carried on by the insurer.
Strategic risk*	Refers to the risk created by an authorized insurer's business strategy. Strategic risk includes risks arising from poor business decisions, substandard execution of decisions, inadequate resource allocation, or a failure to respond well to changes in the business environment.
Stress testing*	Testing which measures the financial impact of stressing one or relatively few factors affecting the authorized insurer.
Systemic risk***	In the context of insurance, the risk of potential negative impact posed by the authorized insurer, which can

	materialize through contagion (where policy holders or markets consider that similar problems may exist in similar products from other insurers) or financial links (for example, through participation in the derivatives markets), negatively affecting the real economy in which the insurer operates. Negative impact on the real economy can be assessed or evidenced, for example, through a failure to make good on promises to policy holders or a failure to engage in new transactions that would foster economic activity.

Sources:

* adapted from IAIS's Glossary or ICP 16, including proposed changes

** https://www.iaisweb.org/page/supervisory-material/issues-papers/file/57927/issues-paper-on-conduct-of-business-risk-and-its-management

*** http://www.iaisweb.org/page/supervisory-material/financial-stability-and-macroprudential-policy-and-surveillance/file/61174/systemic-risk-from-insurance-product-features

Annex A – Identification of Group

For the purpose of identifying "group risk", "group events" and "intra-group transactions" to which an authorized insurer may be exposed or impacted by, the group to which the insurer belongs needs to be identified. For this purpose, the process below should be followed:

(a) As a starting point, the group should include all entities which are treated as being part of the same group to which the authorized insurer belongs, according to the consolidated financial statements in which the authorized insurer is included.

(b) The group should also include any other entity which is linked to the authorized insurer either by way of operational control or another form of common linkage (e.g. common directors, involvement in the policy-making process and material transactions etc.) and where such entity is assessed to pose material contagion risk (whether financial, operational or reputational) to the insurer.

Annex B – Types of notifiable material intra-group transactions or events

Based on the Board's judgement on materiality of the expected impact to the authorized insurer, it should submit prior notification to the IA of the following types of intra-group transactions or events:

Intra-group transactions

- Cross shareholdings
- Loans and receivables
- Guarantees, commitments, and other off-balance sheet exposure
- Arrangements for provision of management or other services (e.g. investment management)
- Risk transfers and capital transfers in whatever form (e.g. inward and outward reinsurance)
- Custodian and nominees services; and
- Purchase or sale of assets.

Events or transactions of the group

- Change of Board members or senior management at holding company level, or at group member level if the group member concerned can exercise significant influence on the insurer
- Major acquisitions and disposals; and
- Establishment of new operating entities.

The list above is non-exhaustive and for general reference only. It aims to help facilitate the Board's judgement and does not exempt the Board's obligations on reporting other types of material intra-group transactions or events not listed above.