GUIDELINE
ON
ENTERPRISE RISK MANAGEMENT

Insurance Authority

1. Introduction

1.1 This Guideline is issued pursuant to section 133 of the Insurance Ordinance (Cap. 41) ("the Ordinance") taking 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 within its risk management system an enterprise risk management ("ERM") framework for solvency purposes to identify, measure, report and manage the insurer's risks in an ongoing and integrated manner.

1.2 The critical objective of this Guideline is to nurture a strong risk culture in the insurance industry that would be reflected in the values, attitudes and norms of business behaviour. The Board and senior management should take ownership in shaping the risk culture of authorized insurers as business practices and decisions are ultimately driven by the risk culture.

1.3 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 the adequate protection of policy holders. An authorized insurer embeds an integrated set of processes and activities within the risk management system established by the insurer for the effective implementation of ERM for solvency purposes.

1.4 This Guideline sets out the supervisory objectives, guidance, and expectations that the Insurance Authority ("IA") would have to assess the overall competence of an authorized insurer's ERM framework and Own Risk and Solvency Assessment ("ORSA"). Insurers should take into account this Guideline and the nature, scale and complexity of risks associated with their business operations in Hong Kong and coordinate their ERM framework and ORSA appropriately.

1.5 A principle-based approach is adopted for this Guideline. This would allow the flexibility for compliance where an authorized insurer considers that it would be more appropriate to deviate from this Guideline having regards to its specific circumstances. In these circumstances, the insurer should explain or demonstrate to the IA's satisfaction that such deviations are appropriate.

2. Application

2.1 Unless specified otherwise by the IA, this Guideline should apply 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 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;

"marine mutual" refers to an authorized insurer which is a mutual company and restricted to insure its members against losses, damages, or liabilities arising out of marine insurance, and whose articles of association, rules or by-laws provides for calling for additional contributions from, or reduction of benefits to, its members; and

"marine insurance" has the meaning assigned to it by section 2 of the Marine Insurance Ordinance (Cap. 329)

Three-tier Group-wide Supervisory Approach

2.2 To achieve effective group-wide supervision and adequate protection to policy holders, the IA adopts a three-tier group-wide supervisory approach ("GWS approach") towards authorized insurers that are being part of larger groups. The GWS approach is detailed in **Annex A**.

2.3 Where an authorized insurer is part of a group, the insurer may rely on the ERM framework or policies of the group provided that the ERM framework or policies of the group is appropriate for the nature, scale and complexity of the risks associated with its business operations in Hong Kong. Otherwise, the insurer should establish a local ERM framework or policies for the Hong Kong operations that observes this Guideline.

2.4 In the context of ORSA, the GWS approach provides flexibility for authorized insurer(s) to structure its ORSA with due regard to the way by which their risks are managed as long as relevant minimum requirements are met:

- Tier 1 refers to those insurance group(s)[1] that is subject to the home supervision of the IA, is required to prepare ORSA on a group-wide basis ("group ORSA");

- Tier 2 refers to those insurance sub-group(s)[2] within an insurance group, with the aggregate of insurance business carried on in or from Hong Kong by all authorized insurers within the sub-group, being significant to the Hong Kong insurance market or to its whole group, is required to prepare ORSA on a sub-group basis ("sub-group ORSA");

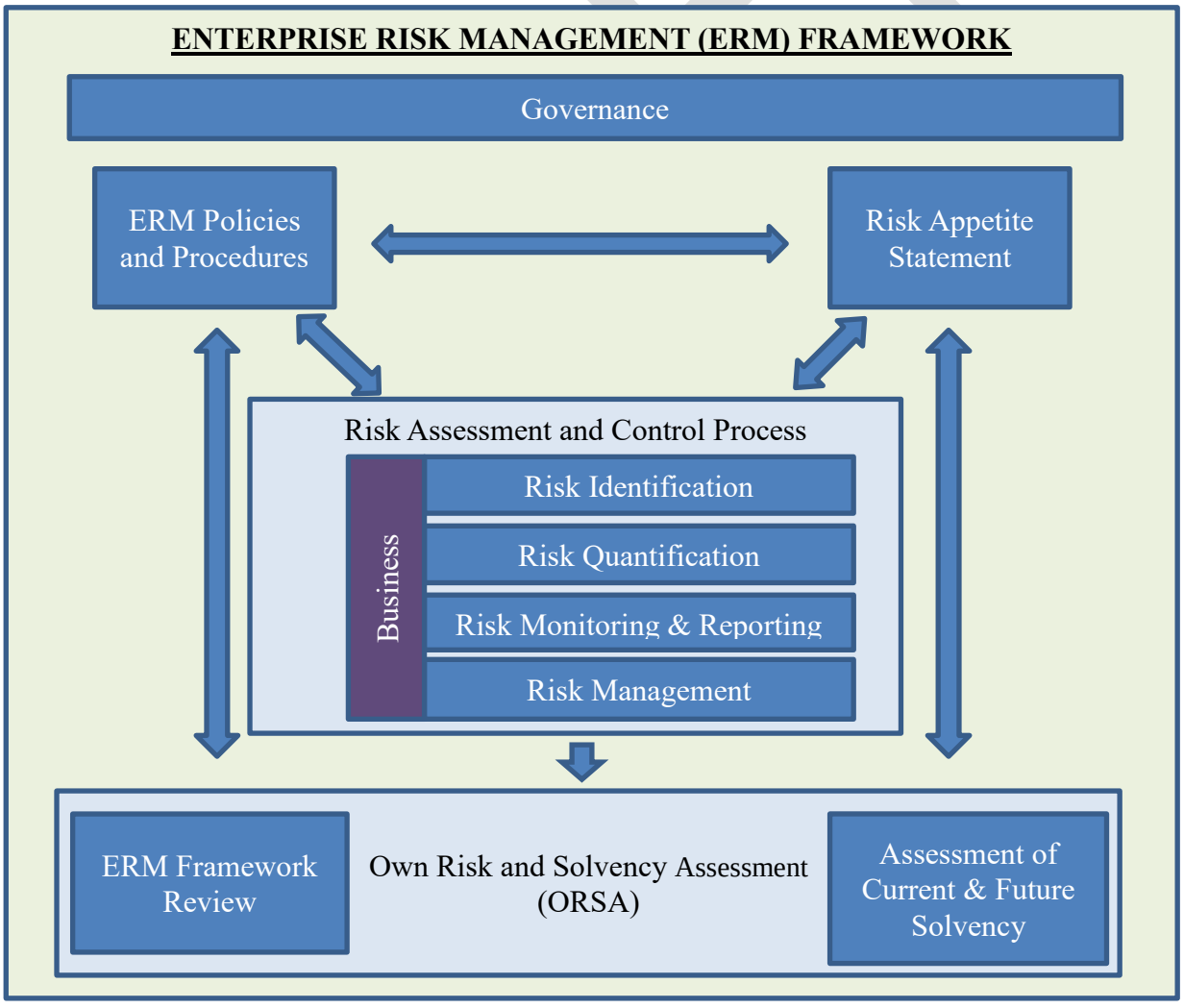
- Tier 3 refers to an authorized insurer(s) that is part of an insurance group and is neither Tier 1 nor Tier 2, is required to prepare ORSA on a solo basis with due consideration on group risk ("solo ORSA with group risk").

2.5 Authorized insurers being part of a larger group would be identified and classified into the above tiers by the IA appropriately. This Guideline sets out the minimum requirements on the ERM *(section 6)* and ORSA *(section 9)* with respect to group or sub-group basis.

[1] [2] Please refer to Glossary for definition.

3. Overview of ERM Framework and General Requirements

3.1 An authorized insurer should have an ERM framework with sufficient governance to ensure safe and sound operation. The ERM framework is the process of identifying, assessing, measuring, monitoring, controlling and mitigating risks in respect of the insurer and, if applicable, the group to which it belongs. It involves setting the risk appetite and the self-assessment of all reasonably foreseeable and relevant material risks that the insurer faces, and their inter-relationships, providing a link between ongoing operational management of risk and longer-term business goals and strategies.



3.2 The board of directors ("Board") of an authorized insurer has the ultimate responsibility to establish, implement and oversee an effective ERM framework, which should consist of:

(a) appropriate governance structure with well-defined roles and responsibilities and reporting lines in order to maintain 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 insurer:

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

The related risk assessment and control processes described should be performed on a regular basis. Such processes could 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 which is a regular assessment of the insurer's current and future risk profile, solvency and liquidity positions, with a review of the effectiveness of the ERM framework *(see section 9)*.

3.3 An authorized insurer should consider the following in establishing and designing the ERM framework, which should be factored in each aspect within the framework and throughout this Guideline:

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

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

(c) forward-looking view with a reasonably long time horizon (which normally covers at least three years) consistent with the nature of the risks, including risks pertaining to the group that may affect the

insurer's operations in Hong Kong and the insurer's business planning horizon;

(d) ability to address material risks[3] and interdependencies, and their potential impact on the business;

(e) a transparent and systematic approach to managing risks according to the risk appetite statement, to maintain liquidity and solvency and manage capital on an ongoing basis; and

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

3.4 There should be proper documentation with regard to the ERM framework on the policies and procedures, breaches, decision-making process, management actions taken, reviews and approvals.

3.5 Where an insurer being part of a larger group, the ERM framework should address group risk and risks should be managed adequately in a cross-border context, if any.

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

4. Governance

Objectives

An authorized insurer should have clear and well-documented risk management policies and procedures in place appropriate for the nature, scale and complexity of the risks associated with the business conducted. 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 Risk Committee or senior management to approve operational procedures.

The ERM governance should be appropriate for the 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 responsibilities, 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 embed a strong risk culture and effective risk management practices throughout the business;

(d) approve and periodically review the risk appetite statement and ensure it is effectively communicated and used throughout the business;

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

(f) understand the risks taken by the business and the approaches taken to control those risks;

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

(h) review and challenge 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 ORSA results as part of its strategic and other business decision-making; and

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

4.2 The Board may delegate part of the ERM activities to the Risk Committee or other competent individuals or committees. However, the Board should retain ultimate responsibility.

Risk Committee

4.3 As provided in 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 authorized insurers) are required to establish a Risk Committee.[4] 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 authorized insurer.[5]

4.4 The Risk Committee has ERM responsibilities to the extent applicable:

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

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

[5] 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) independently review the identification, measurement, monitoring and management of material risks and any areas of non-compliance with the ERM framework;

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

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

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

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

Senior Management

4.6 Senior management has responsibilities for implementing the ERM framework and ensure that:

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

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

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

4.7 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

4.8 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 to the Board, Risk Committee or senior management to establish and implement appropriate policies and procedures in relation to the ERM framework. The scope of support may include solvency, capital and liquidity planning, product management, business planning, reinsurance and risk transfer strategy, ALM and investment strategies.

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 risk appetite statement should be ultimately responsible and approved by the Board. An effective risk appetite statement should be able 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 all relevant and material categories of risk and their interdependencies;

(c) take into account the 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 to the established risk appetite statement or risk limits should be timely reported to the Risk Committee or senior management and, if necessary, escalated to the Board. The Board is expected to approve activities that may deviate from the risk appetite only in rare cases and with good justification.

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 encompass regular risk assessment and control activities:

(a) risk identification;
(b) risk quantification;
(c) risk monitoring and reporting; and
(d) 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 and concentration risks;
- credit default risk;
- liquidity risk;
- operational risk – including legal, compliance, conduct, cyber and reputational risks;
- strategic risk;
- emerging risks – e.g. climate risk; and
- group risk, for insurers being part of a group – including contagion risk.

6.1.2 The risk management policy 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 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 of the nature, scale and complexity of risks:

(a) encompass a sufficiently wide range of techniques, models and scenarios for effective risk and capital management. Stress and Scenario Testing ("SST") 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 regulatory capital requirements; and

(c) be based on a consistent economic assessment of the regulatory and economic capital positions, 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 (and other) circumstances to manage or mitigate the risks, and the timing of such management actions.

Relating Risk to Capital

6.2.3 Being part of the ERM framework and ORSA, an authorized insurer should associate risk assessment with its capital needs. An insurer is generally expected to develop an internal economic capital measure or model[6] based on its own specific circumstances that may cover more widely than the regulatory capital requirements.

6.2.4 Where an insurer prepares internal economic capital measurements, its target level of economic capital needs should be not less than the

[6] The level of sophistication should be commensurate to the nature, scale and complexity of the operations and risks faced.

regulatory capital requirements. The insurer should determine the target level of economic capital that is expected to hold at all times, commensurate with the stated business plans, risk appetite, risk mitigation initiatives, diversification and time horizon.

Use of Models[7] in ERM

6.2.5 Where appropriate, authorized insurers should consider the need for suitable models to facilitate risk quantification, assessments of risk and capital adequacy.[8] The outputs from risk identification stage should guide which material risks should be modeled, and inform any risk interdependencies.

6.2.6 Where a model (internal or external) is used for risk management purpose, an authorized insurer should give consideration to :

(a) the complexity of the model that should commensurate with the undertaken risks;

(b) the expertise required in complex modelling activities;

(c) the basis for valuation of assets and liabilities, risk measures, target level of confidence and the time horizon of the model outputs;

(d) modeled stresses and scenarios that are sufficiently adverse and plausible;

(e) the regulatory and economic capital associated with each material risk and the capital planning period; and

(f) internal models calibrated according to own modelling criteria that is appropriate to its risk strategy and business plans.

6.2.7 The 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.

6.2.8 The models used should be consistently embedded in decision-making and risk management of the business.

[7] "Modelling" in this context does not necessarily mean complex stochastic modelling. It can also include less sophisticated methods.

[8] For example, internal models may be used for insurer-specific risks, while external models may be used for market or catastrophe risk.

6.2.9 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 validation such as back-testing regularly. Independent review and validation is encouraged to ensure objectivity.[9]

Stress and Scenario Testing

6.2.10 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.

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

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

(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;

(d) likely quantitative and qualitative impacts to the insurer within the modeled stresses and scenarios. The modeled management actions required e.g. at portfolio level, solo level or group/sub-group level should be objective, realistic, achievable, adequate and legal.

[9] For example, the personnel responsible for the review and validation is not the one who designs or owns 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.

[11] Development of own scenarios could be referenced to pandemic scenario, catastrophic events, sovereign default, severe economic recession, global financial crisis, mass policy holder surrenders, etc that are justified as relevant to the authorized insurer.
For non-quantifiable or operational risks such as legal, reputational, conduct, and cyber risks, an authorized insurer should consider assessment through the use of 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 and/or capital to movements in, for example, lapses, claims, interest rates, etc either over a short or long period of time.

6.2.12 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 ORSA.

6.2.13 The details (e.g. key assumptions and limitations in constructing the stresses and scenarios) and outcomes of SSTs, together with the corresponding management actions are expected to be concisely presented in the ORSA Report (please refer to paragraphs 9.3 to 9.5 for relevant details).

Continuity Analysis

6.2.14 Based on the nature, scale, and complexity of the business operations, an authorized insurer should give consideration to conduct 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 regulatory capital requirements.

6.2.15 Continuity analysis may address the following specific to the authorized insurer, to the extent applicable:

(a) a combination of qualitative and quantitative elements in the medium and longer-term business strategy, projection of future financial position and analysis of the insurer's ability to meet 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 or recovery plans (see considerations in paragraph 6.4.4) for use in a going- and gone-concern situations to restore financial strength and viability.

Business Failure Analysis

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

6.2.17 The use of reverse stress testing ("RST")[13] 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 capital fungibility, 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:

(a) identifying the sources and causes of risks;

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

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

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

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

(f) being conducted in a clear and concise manner yet comprehensive enough to facilitate informed decision-making; and

(g) being included into the ORSA Report (see *section 9* for detailed requirements).

[13] Depending on the nature, size and complexity of the insurers and risks it faces, RST could be performed through quantitative modelling, qualitative analysis, or hybrid approach.

6.3.3 Risk monitoring and reporting should cover all 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 identify reporting and procedures explaining data errors or weaknesses.

6.3.5 The Board and senior management should periodically review that the information, in terms of both amount and quality, remains relevant and appropriate to risk governance, risk management process and risk appetite, and 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 Management Review and Actions

6.4.1 The ERM framework should enable well-informed business decisions and risk management actions. The identification and quantification of risks should ensure appropriate and timely management actions are taken at the group/sub-group level, solo level, or other appropriate levels, 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 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 may address the following specific to the authorized insurer, to the extent applicable:

(a) the relevant entities and their interconnectedness;

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

(c) a quantitative and qualitative trigger framework in which recovery options are triggered in face of a range of severe adverse situations;

(d) an assessment on the timeliness and creditability of the recovery options[14] 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; and

(f) 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 proper approval process on the management actions at Board level or senior management level, where appropriate.

6.5 Requirements in ERM Processes for Groups

6.5.1 The ERM framework of Tier 1, 2 and 3 groups should meet the following minimum requirements in respect of group risk.

6.5.2 From the authorized insurer's perspective, the relevant Board and senior management should ensure appropriate coordination with the head of its group or the other individual group entities when setting the risk management policies of the insurer and any possible differences with group policies should be identified.

6.5.3 The ERM framework 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 an impact on the authorized insurer. The ERM framework should take into account relevant material

[14] 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.

risks arising from insurance and non-insurance entities (regulated or unregulated) and partly-owned entities of the group that may impact the insurer.

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

6.5.5 The ERM framework should give consideration to the risk that the support of the insurer by group entities may not be available when there is a concern about another part of the group. Dependent on own circumstances, this may entail monitoring, setting quantitative and qualitative restrictions and reporting significant group events and intra-group exposures, as appropriate.

Additional Requirements in ERM Processes for Tier 1 Groups

6.5.6 In addition to paragraphs 6.5.1 to 6.5.5, Tier 1 group should have risk management policies to address material risks at both group and solo levels. Where relevant, the group-wide ERM framework should give consideration to cover, among others, the risks listed in paragraph 6.1.1 and to the management of these risks in a cross-border context.

6.5.7 The Board of the Tier 1 group is responsible for ensuring the effectiveness of the group-wide ERM framework (see paragraph 8.2.2 for relevant ERM Framework review requirements). Senior management should apply measurement techniques that are appropriate and adequate to the group-level.

6.5.8 The group-wide ERM framework should be updated where there is any material change to the group structure or strategy.

6.5.9 Within the group, there should be sufficient coordination and exchange of information between the group and its entities as part of their respective feedback loops to ensure relevant changes in risk profiles have been taken into account.

6.5.10 In addition, the Board of the group should ensure that the group-wide ERM framework be integrated with their organizational structure,

decision-making processes, business operations, and should give consideration to the following:

(a) risk exposure of the group against the group-wide risk appetite and risk limits structure on an on-going basis;

(b) diversity of activities of the group;

(c) nature and degree of risk of individual legal entities or business lines;

(d) cumulative risks at the group level, in particular risks in a cross-border context and intra-group reinsurance;

(e) effectiveness of reinsurance and risk transfer arrangements of the group in adverse circumstances;

(f) interconnectedness of the legal entities within the group;

(g) sophistication and functionality of information and reporting systems in addressing key group-wide risks; and

(h) laws and regulations of the jurisdictions where the group entities operate.

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 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. [15] 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, the authorized insurer should also develop and maintain other risk management policies, including where relevant and material:

- 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 and the corresponding guidance in paragraphs 7.4 to 7.14 are neither exhaustive nor mandatory. Authorized insurers should design their ERM framework in accordance to their own specific circumstances.

[15] In the case of product life-cycle, it 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.

7.4.2 The underwriting policy should address the approaches and controls taken that give consideration to the:

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

(b) identification of underwriting risks and preferably include emerging risks;

(c) quantification of underwriting risk, and in relation to the economic and regulatory capital requirements;

(d) monitoring and reporting of underwriting risks;

(e) mitigation and control of underwriting risks;

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

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

7.4.3 The underwriting policy should ensure that the impact on economic and regulatory capitals is considered whenever there is an anticipated material change to the underwriting risks accepted by the insurer.

7.4.4 Where appropriate, independent professional valuation or advice should be sought for an assessment of the risks covered in the underwriting process.

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 taken that give consideration to:

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

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

(d) 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 economic and regulatory capital;
- 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 investment activities. Authorized insurers are required to observe the Guideline on Asset Management by Authorized Insurers ("GL13").

7.6.2 The investment policy of an authorized insurer should identify appropriate controls to ensure, to the extent applicable:

(a) capacity to bear investment risk, appropriate for its risk appetite statement and risk limits structure, types of business, capital and liquidity needs;

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

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

(g) how investment strategies and allocation being considered with economic and regulatory capital;

(h) any engagements of investment tools such as derivatives should be closely monitored; and

(i) minimization of legal and basis risks; and

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

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

7.6.4 Policy holder funds should be prudently managed. Where appropriate, there should be procedures including but not limited to:

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

(b) maintenance of 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. [16]

7.7.2 The reinsurance and risk transfer policy of an authorized insurer should address the approaches and controls taken that give consideration to the:

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

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

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

(e) how reinsurance and risk transfer strategies are considered with economic and regulatory capital;

(f) 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

[16] Authorized insurers are also required to observe Guideline on Reinsurance ("GL17") issued by the IA.

(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 arrangement 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.

7.8.3 The liquidity policy of an authorized insurer should address the approaches and controls taken that give consideration to the:

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

(b) 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 liquidity risk policy.

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 should be capable of evaluating and providing advice regarding, 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 taken that give consideration to the:

(a) methodologies, models and assumptions used in calculations of solvency position, regulatory capital requirements, technical provisions, reserving, 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) actuarial-related risk modelling in the ORSA;

(e) monitoring and reporting of actuarial-related risks; and

(f) 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 the trend of court awards or other applicable considerations. As such, it is essential for the 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.

7.10 *Conduct Risk*

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. 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 extended to those functions or activities that are outsourced.

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

7.11 *Cyber Risk*

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.

7.11.2 The cyber risk policy of an authorized insurer should address the approaches and controls taken that give consideration to the:

(a) protection of the personal information of its policy holders, and digital or electronic data of its business to ensure continuity of the business operations;

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

(c) identification of cyber security threats arising from network, attacks, phishing activities, relevant devices and so on;

(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 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.

7.13 *Internal Controls*

7.13.1 The ERM framework should include a risk management policy on internal controls (or internal controls policy), as appropriate, to ensure systems[17] and functions are adequate for the authorized insurer's objectives, strategies, risk profile, and the applicable legal and regulatory requirements, and adaptable to internal and external changes.

7.13.2 The internal controls policy should address the approaches and controls taken that give consideration to the:

(a) internal controls activities relevant to the key activities, critical IT functionalities, access to critical IT infrastructure by staff and related third parties, and important legal and regulatory obligations of the insurer;

(b) procedures to identify potential suspicious transactions[18];

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

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

(e) regular review of internal controls policy, systems and activities.

7.13.3 Effective channels of communication 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.

[17] "Systems" here include the strategies, policies, processes and controls in place.

[18] This is **not** restricted to authorized insurer that carries on long term business which is required to observe 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., could be in place to ensure checks and balances with clear and well defined reporting line.

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 ensure data is current, accurate and complete; and protect 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 taken that give consideration to the:

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

(b) safeguards against operational risk events such as theft of data, breach on disclosure of sensitive data, 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 and systems and policy.

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

8. ERM Framework Review

Objectives

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

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 and should have 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 by a suitably experienced individual who reports directly to or is a member of the Board.

8.2.2 In particular for Tier 1 group(s), the ERM framework should be reviewed by an independent party[19] at least every three years, in order to ascertain that the ERM framework remains fit for purpose and the review results should be incorporated in the ORSA Report.

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 reasonable frequency. The validation may, as appropriate, include the underlying

[19] The ERM framework review may be carried out by an internal or external body as long as the reviewer is independent and not responsible for, nor been actively involved in, the part of the ERM framework that it reviews.

assumptions of the SSTs, the sufficiency of the severity of the SSTs, 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 the 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, **at minimum**, an ORSA at solo level ("solo ORSA"). The IA expects the outcome of the ORSA in the form of a report ("ORSA Report") that gives consideration to the minimum requirements in paragraph 9.5 on solo level and paragraph 9.6 on group or sub-group level, as applicable.

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

9.2 For authorized insurers being part of a group, these insurers should also consider group risk and perform ORSA at the level consistent with the way their operations and material risks are managed.

9.2.1 Subject to IA's approval **(**See **Annex A)** and meeting the minimum requirements, Tier 1 and Tier 2 groups that manage risks on a group or sub-group basis, may opt to prepare a single or separate ORSA Report(s) that cover the group or sub-group level **and** the solo-level for each authorized insurer.

9.2.2 The entities that should be covered in the ORSA Report for the Tier 1 and Tier 2 are different, i.e. the Tier 1 covers all entities of the insurance group while the latter covers only the authorized insurers of the Tier 2 sub-group.

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 insurer, so that the ORSA continues to provide relevant information for decision making at the Board, Risk Committee, senior management or risk management control function levels.

Minimum Requirements of ORSA Report at solo level

9.4 The ORSA should encompass the following in a concise manner:

(a) all activities of the regular cycle of risk assessment (described in sections 5, 6 and 7) that includes an analysis of key drivers of the change in the financial, economic and capital adequacy positions, summary of methodologies to determine the capital for regulatory and economic purposes; and

(b) a review of the effectiveness of the ERM framework (described in section 8)

9.5 The solo ORSA undertaken by an authorized insurer should be appropriate to the nature, scale and complexity of its risk. It should include, but not be limited to, the following:

(a) the risk appetite statement;

(b) the year-on-year key changes in the ERM framework;

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

(d) the considerations for each foreseeable and relevant material risk. It should explicitly state those risks that are quantifiable and those that are not quantifiable;

(e) a description of the models used to identify and assess risks, the risk limits structure, and the economic capital needed to meet those risks; the modelling criteria used to determine the economic capital, including basis for valuation of the assets and liabilities and the confidence level, risk measure and time horizon;

(f) the summary of the quantitative and/or qualitative risk assessments in both normal and adverse situations for each material risk;

(g) the assessments of the regulatory capital and economic capital needed given the risk appetite and business plans and the risk management actions;

(h) reasons attributed to differences between the actual and planned, regulatory and economic capital outcomes;

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

(j) the SST results, including the impacts on regulatory and economic capital, on both IA prescribed scenarios and insurer's own scenarios with details of management actions and their impact with explanation and justification:

- For long term insurance business, the insurer should, besides applying stresses or scenarios relevant to its business operations, use the scenarios provided in the Actuarial Guidance Note 7 on Dynamic Solvency Testing ("AGN7") issued by the Actuarial Society of Hong Kong; and

- For general insurance business, the insurer should consider, at minimum, the adverse changes in (i) claims experience, (ii) claims inflation, and (iii) default of major reinsurer(s) and their interconnectedness;

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

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

(m) if any, the recovery plan and the assessments of the recovery options.

Additional Requirements of ORSA Report for Tier 1 and Tier 2 Groups

9.6 In addition to the solo ORSA requirements listed in paragraph 9.5, Tier 1 and Tier 2 groups should give consideration to the following requirements when performing or extending the ORSA on a group-wide basis (i.e. group ORSA) or, **where applicable to**, sub-group basis (i.e. sub-group ORSA):

(a) legal and management structures and practices at the group or sub-group level, and thus the entities being covered under the group or sub-group ORSA;

(b) risk aggregation results, including the approaches to correlation and diversification;

(c) material risks arising from non-insurance entities (regulated or unregulated) and partly-owned entities within the insurance group or sub-group;

(d) non-quantifiable risks which are important to consider at group or sub-group perspective;

(e) group or sub-group-wide economic capital models;

(f) liquidity, solvency and capital adequacy of each entity of the insurance group or sub-group and the insurance group or, if applicable, sub-group as a whole from regulatory and economic capital viewpoints;

(g) financial or other activities being undertaken by individual entities that might change the risk profile of the insurance group or sub-group;

(h) transferability of assets and fungibility of capital across entities within the group or sub-group;

(i) business strategy evidenced by significant or unusual growth or shifts in business volumes, new lines of business or operations in new jurisdictions;

(j) risks posed from the involvement in non-traditional non-insurance ("NTNI") activities and exposures to the systemic risks of failure;

(k) group or sub-group level SSTs that impact current and future financial conditions and describe the management actions at the relevant level; and

(l) group or sub-group level continuity analysis that focuses on the ability to continue to exist as an insurance group or sub-group, and outline management actions to manage potential cash flow implications and distribution of capital in the insurance group or sub-group in a stress scenario(s).

10. Reporting to the Insurance Authority and Supervisory Review

10.1 All authorized insurers which are subject to this Guideline are required to submit their ORSA Report annually to the IA within four months after each financial year end, and whenever there are material changes in the risk profile. The IA requires approval of the ORSA Report at the Board or Risk Committee level. Deliberations on the ORSA outcome should be minuted for supervisory review.

10.2 An authorized insurer that is part of a group is required to submit, as permitted by applicable law, regulations and rules, prior notification 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 transactions to the IA promptly in written form. Examples of notifiable intra-group transactions or events are detailed in **Annex B**.

The prior notification to the IA is not an approval process. It facilitates the IA to monitor possible group risk, interconnectedness of group entities and their potential impact on solvency, liquidity and profitability.

10.3 ***Supervisory Review and Expectations***

10.3.1 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 and substance over form in the reviews. 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.

10.3.2 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 the business decision or risk management on considerations of the economic capital, regulatory capital requirements, 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) review the effectiveness of the ERM framework by an independent party; and

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

11. Implementation

11.1 This Guideline would take effect from [1 January 2020].

11.2 Authorized insurers should lodge to the IA its first ORSA Report for the financial year ended [on or after 31 December 2020] within four months after the end of the financial year.

Glossary

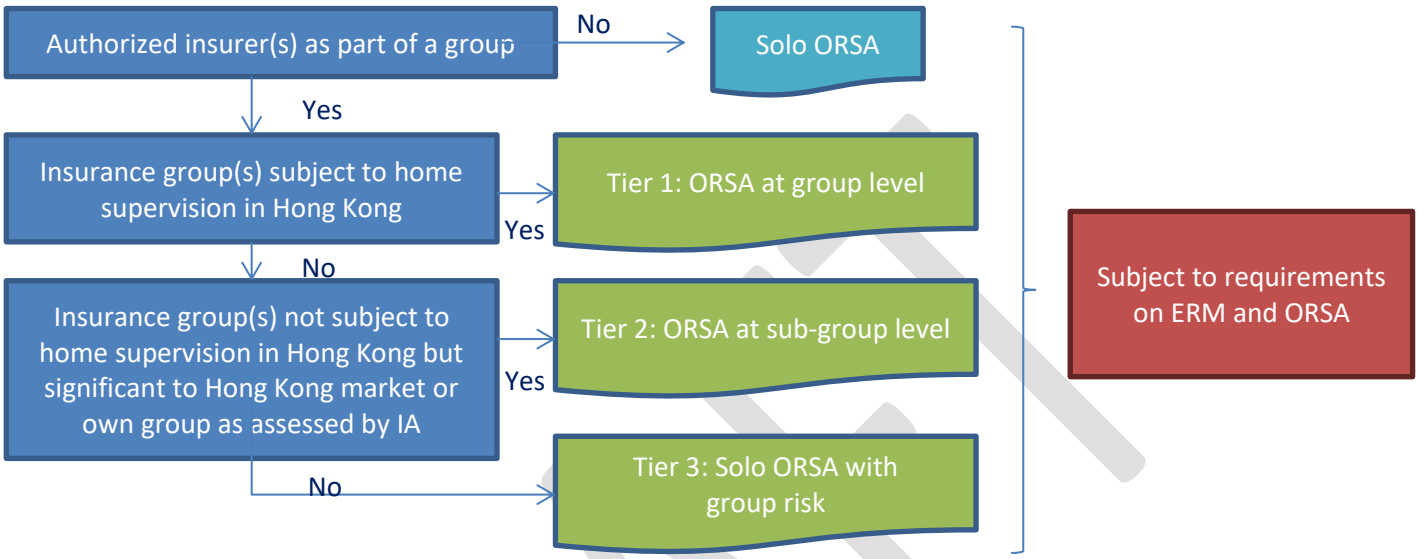
Capital Adequacy*	The adequacy of capital resources relative to regulatory capital requirements.
Capital Resources*	Financial resources that are capable of absorbing losses.
Economic Capital*	The capital needed by the authorized insurer to satisfy its risk tolerance and support its business plans and which is determined from an economic assessment of the insurer's risks, the relationship between them and the risk mitigation in place. An insurer's assessment of economic capital may therefore be different to their assessment of regulatory capital.
Group Risk*	Group risk arises for an authorized insurer that is a member of a group or is an insurance group or sub-group. Group risk includes the risk that the insurer or insurance group or sub-group may be adversely affected by an occurrence (financial or non-financial) in another group entity or of the wider group. Group risk also includes the risk that the financial stability of an insurer within a group or an insurance group or sub-group may be adversely affected by an event in a legal entity within the group or sub-group, a group-wide occurrence or an event external to the group or sub-group.
Insurance Group*	Two or more legal entities, at least one of which is an insurance legal entity, where one has control over one or more insurance legal entities and possibly other non-regulated legal entities, and whose primary business is insurance.
Insurance Sub-group	For the purpose of this Guideline, it consists of at least two or more authorized insurers that are part of an insurance group, and share ERM framework and processes that are subject to the same governance.

Key person(s) in risk management / actuarial control functions	Is 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, in relation to an authorized insurer.
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. It 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.
Regulatory Capital*	Surplus of assets over liabilities, evaluated in accordance with the Insurance Ordinance (Cap.41).
Reverse Stress Testing*	Identifies scenarios that are most likely to cause an authorized insurer or insurance group to fail, and focus 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 account of regulatory capital requirement, 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*	Risk Limits structure is the aggregate set of authorized insurer's self-imposed limits 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*	Scenario testing considers the impact of a combination of circumstances to reflect extreme historical scenarios which are then analyzed in light of current conditions. Scenario testing may be conducted deterministically or stochastically.
Senior Management	Refers to individuals, headed by the chief executive, responsible for managing the business of an authorized insurer on a day-to-day basis in accordance with strategies, policies and procedures set out by the board of directors.
Stress Testing*	Stress testing measures the financial impact of stressing one or relatively few factors affecting the authorized insurer.

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

Annex A – Three-tier group-wide supervisory ("GWS") approach



A.1 The IA adopts the three-tier GWS approach, where:

(a) ***Tier 1*** refers to insurance group(s) that is subject to *de facto* home supervision of IA on a group-wide basis, i.e. IA imposes group-wide supervision, group-wide regulatory requirements and group-wide supervisory review and reporting. Thus, Tier 1 groups would be subject to prescribed capital requirements at group level and solo level; corporate governance, ERM and ORSA requirements; and prior notification requirement of group events and intra-group transactions that are material to the authorized insurers within the group or to the overall group.

(b) ***Tier 2*** refers to authorized insurer(s) being part of a wider group ("sub-group") which is significant to the Hong Kong insurance market or to its own group but not subject to home supervision of IA on a group-wide basis. As compared to Tier 1, IA's regulatory focus covers mainly Hong Kong authorized insurers within the sub-group and the risk management assessment by the group or sub-group on those Hong Kong authorized insurers. Tier 2 groups would be subject to corporate governance, ERM and ORSA requirements, and prior notification requirement of group events and intra-group transactions that are material to the insurer or to the sub-group.

For clarity, Tier 2 groups are not subject to prescribed capital requirements at sub-group level.

(c) For a ***Tier 2 group***, the IA's decision in determining the significance to the Hong Kong insurance market or to its own group would be based on:

A. ***Significance to Hong Kong market*** is referenced to the aggregate premium of inforce business or aggregate liabilities, attributable to Hong Kong insurance business; or systemic influence on the Hong Kong market.

B. ***Significance to its own group*** is referenced to the aggregate premium of inforce business or aggregate assets under management or aggregate liabilities, attributable to Hong Kong insurance business as compared with that of global business; or critical functions in Hong Kong which is vital to the operation of its own group.

(d) ***Tier 3*** refers to authorized insurer(s) being part of a wider group and is neither *Tier 1* nor *Tier 2*. Each Tier 3 insurer would be subject to IA's applicable prescribed capital requirement, ERM and ORSA requirements at the solo level, and prior notification requirement of group events and intra-group transactions that are material to the insurer.

A.2 ***Submission options for ORSA of a Tier 1 or Tier 2 group***

The IA gives due regard to the various corporate and risk management structures of Tier 1 and Tier 2 groups in Hong Kong. ***Upon the authorized insurer's application and subject to IA's approval***, Tier 1 and Tier 2 groups are given the flexibility to structure its ORSA submissions by which their risks are managed as long as relevant minimum requirements on ERM and ORSA in this Guideline are met.

Annex B – Reportable types of material intra-group transaction or event

This non-exhaustive list is for reference to facilitate the Board's judgement only and does not exempt the Board's obligations on reporting other types of material intra-group transaction or event.

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

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. 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.