



IAIS

INTERNATIONAL ASSOCIATION OF
INSURANCE SUPERVISORS

Public

INSURANCE CORE PRINCIPLES, STANDARDS, GUIDANCE AND ASSESSMENT METHODOLOGY

Revised ICP 8 and the additional ComFrame material in ICP 8 for public consultation (redline version)

This public consultation focuses on changes made to ICP 8 aimed at removing overlaps and duplications between ICP 8 and ICP 16 (in track changes in the redline version). For this reason, only relevant parts of ICP 8 are included in the consultation document. A full text of ICP 8 and other ICPs is available [here](#). The ComFrame material integrated with ICP 8 that was released for consultation in March 2017 is not open for additional consultation at this stage; it is still under review based on the comments received during that consultation. Since the March 2017 consultation, additional ComFrame material has been integrated with ICP 8. This new material, which is in track changes, is subject to public consultation (full version of the ComFrame material released for consultation in March 2017 is available [here](#)).

ICP 8 Risk Management and Internal Controls

The supervisor requires an insurer to have, as part of its overall corporate governance framework, effective systems of risk management and internal controls, including effective functions for risk management, compliance, actuarial matters and internal audit.

Introductory Guidance

- 8.0.1 As part of the overall corporate governance framework and in furtherance of the safe and sound operation of the insurer and the protection of policyholders, the Board is ultimately responsible for ensuring that the insurer has in place effective systems of risk management and internal controls and functions to address the key risks it faces and for the key legal and regulatory obligations that apply to it. Senior Management effectively implements these systems and provides the necessary resources and support for these functions.
- 8.0.2 In some jurisdictions, risk management is considered a subset of internal controls, while other jurisdictions would see it the other way around. The two systems are in fact closely related. Where the boundary lies between risk management and internal controls is less important than achieving, in practice, the objectives of each.
- 8.0.3 The systems and functions should be adequate for the insurer's objectives, strategy, risk profile, and the applicable legal and regulatory requirements. They should be adapted as the insurer's business and internal and external circumstances change.
- 8.0.4 The nature of the systems that the insurer has is dependent on many factors. The systems typically include:
- strategies setting out the approach of the insurer for dealing with specific areas of risk and legal and regulatory obligation;
 - policies defining the procedures and other requirements that members of the Board and employees need to follow;
 - processes for the implementation of the insurer's strategies and policies; and
 - ~~and~~ controls to ensure that such strategies, policies and processes are in fact in place, are being observed and are attaining their intended objectives.
- 8.0.5 An insurer's functions (whether in the form of a person, unit or department) should be properly authorised to carry out specific activities relating to matters such as risk management, compliance, actuarial matters and internal audit. These are generally referred to as control functions.

Special considerations for groups

- 8.0.6 Group wide risks may affect insurance legal entities within a group, while risks at the insurance legal entity level could also affect the group as a whole. To help address this, groups should have strong risk management and compliance culture across the group and at the insurance legal entity level. Thus, in addition to meeting group governance requirements, the group should take into account the obligations of its insurance legal entities to comply with local laws and regulations.
- 8.0.7 How a group's systems of risk management and internal controls are organised and operate will depend on the governance approach the group takes, i.e., a more centralised or a more decentralised approach (see IAIS Issues Paper on Approaches to Group Corporate Governance; impact on control functions, October 2014). Regardless of the governance approach, it is important that effective systems of risk management and internal controls exist and that risks are properly monitored and managed at the insurance legal entity level and on a group-wide basis.
- 8.0.8 Additionally, a group's governance approach will also affect the way in which its control functions are organised and operated. Coordination between the insurance legal entity and group control functions is important to help ensure overall effective systems of risk management and internal controls. Regardless of how the group control functions are organised and operated, the result should provide an overall view of the group-wide risks and how they should be managed.
- 8.0.9 Supervisors should require the establishment of comprehensive and consistent group governance and assess its effectiveness. While the group-wide supervisor is responsible for assessing the effectiveness of the group's systems of risk management and internal controls, the other involved supervisors undertake such assessments on a legal entity basis. Appropriate supervisory cooperation and coordination is necessary to have a group-wide view and to enhance the assessment of the legal entities.

Systems for risk management and internal controls

8.1 The supervisor requires the insurer to establish, and operate within, an effective and appropriately documented risk management system⁷, which includes, at a minimum:

- a risk management strategy that defines the insurer's risk appetite;
- a risk management policy outlining how all material risks are managed within the risk appetite; and
- the ability to respond to changes in the insurer's risk profile in a timely manner.

Basic components of a risk management system

- 8.1.1 The risk management system is designed and operated at all levels of the insurer to allow for the identification, assessment, monitoring,

mitigation and reporting of all risks of the insurer in a timely manner. It takes into account the probability, potential impact and time horizon of risks.

8.1.2 An effective risk management system ~~typically includes elements such as~~should:

- ~~a clearly defined and well documented risk management strategy, which includes a clearly defined risk appetite and takes~~take into account the insurer's overall business strategy and ~~its~~ business activities (including any business activities which have been outsourced);
- provide that the insurer's risk appetite, expressed in a risk appetite statement, be used in the insurer's business strategy and embedded in its day-to-day operations;
- provide relevant objectives, key principles and proper allocation of responsibilities for dealing with risk across the business areas and business units of the insurer;
- provide a documented process defining the Board approval required for any deviations from the risk management strategy or the risk appetite and for settling any major interpretation issues that may arise;
- ~~appropriate documented policies that include a definition and categorisation of~~define and categorise material risks (by type) to which the insurer is exposed, at both insurance legal entity and group level where applicable, and the levels of acceptable risk limits for each type of these risk;
- include documented policies that describe the risk standards and the specific obligations of employees and the businesses in dealing with risk, including risk escalation and risk mitigation tools;
- provide suitable processes and tools (including stress testing and, where appropriate, models) for identifying, assessing, monitoring and reporting on risks. Such processes should also cover contingency planning;
- provide for regular reviews of the risk management system (and its components) to help ensure that necessary modifications and improvements are identified and made in a timely manner; and
- appropriately address ~~attention to~~ other matters related to risk management for solvency purposes set out in ICP (16 Enterprise Risk Management for Solvency Purposes); ~~and an effective risk management function.~~

Scope and embedding of the risk management system

- 8.1.3 The risk management system should at least cover underwriting and reserving, asset-liability management, investments, liquidity and concentration risk management, operational risk management, conduct of business, and reinsurance and other risk-mitigation techniques.
- 8.1.4 The risk management system should be aligned with the insurer's risk culture and embedded into the various business areas and units with the aim of having the appropriate risk management practices and procedures embedded in the key operations and structures.

Identification

- 8.1.5 The risk management system should take into account all reasonably foreseeable and relevant material risks to which the insurer is exposed, both at the insurer and the individual business unit levels. This includes current and emerging risks.
- 8.1.6 Significant new or changed activities and products that may increase an existing risk or create a new type of exposure should be subject to appropriate risk review and be approved by the Board and Senior Management.

Assessment

- 8.1.7 Insurers should assess material risks both qualitatively and, where appropriate, quantitatively. Appropriate consideration should be given to a sufficiently wide range of outcomes, as well as to the appropriate tools and techniques to be used. The interdependencies of risks should also be analysed and taken into account in the assessments.
- 8.1.8 [The documentation supporting the insurer's assessment of risk should provide appropriately detailed descriptions and explanations of the risks covered, the approaches used, and the key assumptions made.](#)

[CF8.1a The group-wide supervisor requires the IAIG to reflect, in the documentation of the IAIG's risk management system, differences in risk management that may apply to different legal entities within the IAIG, due to the nature, scale and complexity of the risks associated with business conducted locally.](#)

[CF8.1a.1 The documentation should include explanations of the respective approaches to, or assumptions of, risk management applied across the IAIG and the rationale as to the risk appetite for different individual entities within the IAIG.](#)

[CF8.1a.2 The IAIG should document the methodologies, key assumptions and limitations related to its stress testing and scenario analysis.](#)

Monitoring

- 8.1.9 The risk management system should include [processes and tools for monitoring risk, such as](#) early warnings or triggers that allows timely

consideration of, and adequate response to, material risks. An insurer may decide to tolerate a risk, when it is acceptable within the risk appetite that has been set.

Mitigation

- 8.1.10 The risk management system should include strategies and tools to mitigate against material risks. In most cases an insurer will control or reduce the risk to an acceptable level. Another response to risk is to transfer the risk to a third party. If risks are not acceptable within the risk appetite and it is not possible to control, limit or transfer the risk, the insurer should cease or change the activity which creates the risk.

Reporting

- 8.1.11 Risks, the overall assessment of risks and the related action plans should be reported to the Board and/or to Senior Management, as appropriate, using qualitative and quantitative indicators and effective action plans. The insurer's documented risk escalation process should allow for reporting on risk issues within established reporting cycles and outside of them for matters of particular urgency.
- 8.1.12 The Board should have appropriate ways to carry out its responsibilities for risk oversight. The risk management policy should therefore cover the content, form and frequency of reporting that it expects on risk from Senior Management and each of the control functions. Any proposed activity that would go beyond the Board-approved risk appetite should be subject to appropriate review and require Board approval.

Risk Management Policies

- ~~8.1.13 The insurer's risk policies should be written in a way to help employees understand their risk responsibilities. They should also help explain the relationship of the risk management system to the insurer's overall corporate governance framework and to its corporate culture. The overall risk management policy of the insurer should outline how relevant and material risks are managed. Related policies should be established, either as elements of the risk management policy, or as separate sub-policies. At a minimum, these should include policies related to the risk appetite framework, an asset-liability management policy, an investment policy, and an underwriting risk policy.~~

~~Regular internal communications and training on risk policies should take place.~~

- 8.1.13 The insurer's risk management policy should outline how all material categories of risk are managed, both in the insurer's business strategy and its day-to-day activities. An insurer's risk management policy typically includes a description of the insurer's approach towards risk retention and strategies for risk management, such as the use of reinsurance and derivatives, and degree of diversification/specialisation. It should also clearly address the relationship between pricing, product development and investment management in order for product design

and pricing and the accompanying investment strategy to be appropriately aligned. In particular, the insurer may need to establish investment and product benchmarks to help ensure that it continues to meet its financial objectives. At a minimum, these risk management policies should address the insurer's risk appetite, asset-liability management, investment, and underwriting risk.

8.1.14 The insurer's risk management policies should be written in a way to help employees understand their responsibilities regarding risk management. They should also help explain how the risk management system relates to the insurer's overall corporate governance framework and its corporate culture. Regular internal communications and training within the insurer on risk management policies and risk appetite may help in this regard.

8.1.148.1.15 For insurance groups, a risk management policy addresses the way in which the group manages risks that are material at the insurance group level, including risks that arise from the insurance group being part of a wider group. For an insurance legal entity that is part of a group, the risk management policy of that entity should address management of risks material at the entity level as well as additional risk it faces as a result of its membership in a group, which can encompass the widest group of which the insurance legal entity is a member and not only the entity's insurance group. Within an insurance group, the head of the group and the legal entities should ensure appropriate coordination and consistency between the head of the group and the legal entities when setting risk management policies. Consistency within a group may encompass vertical consistency (between group and legal entity level) as well as horizontal consistency (between legal entities within the group). Both perspectives should lead to the same effect of consistent risk management policies across the group.

CF8.1b4a The group-wide supervisor requires the Head of the IAIG to **ensure establish, and operate within, an appropriately documented and effective** ~~that the~~ risk management system ~~that~~ operates at all levels of the IAIG and covers, at a minimum, the:

- diversity of activities of the IAIG;
- nature and degree of risk of individual legal entities or business lines;
- cumulative risks at the level of the IAIG, in particular cross-border risks;
- interconnectedness of the legal entities within the IAIG;
- sophistication and functionality of information and reporting systems in addressing key group-wide risks; and
- laws and regulations of the jurisdictions where the IAIG operates.

CF8.4a1b.1 The IAIG's risk management system should:

- be integrated with its organisational structure, decision-making processes, business operations, legal entities and risk culture; and
- measure the risk exposure of the IAIG against the risk appetite limits on an on-going basis in order to identify potential concerns as early as possible.

CF8.4a1b.2 The Head of the IAIG should ensure that a risk assessment is carried out before the IAIG enters into new business lines and products and that ongoing risk assessment is carried out after entering into new business areas. The Head of the IAIG should have in place adequate processes, controls and systems to manage the risks of new products.

Changes to the risk management system

~~8.1.15~~ 8.1.16 Both the Board and Senior Management should be attentive to the need to modify the risk management system in light of ~~new internal or external circumstances~~ changes in the insurer's risk profile as well as other new internal or external events and/or circumstances. The risk management system should include mechanisms to incorporate new risks and new information related to risk already identified on a regular basis. The risk management system should also be responsive to the changing interests and reasonable expectations of policyholders and other stakeholders.

~~8.1.16~~ 8.1.17 Material changes to an insurer's risk management system should be documented and subject to approval by the Board. The reasons for the changes should be documented. Appropriate documentation should be available to internal audit, external audit and the supervisor for their respective assessments of the risk management system.

CF8.1c4b The group-wide supervisor requires the Head of the IAIG to review annually the risk management system to ensure that emerging risks are taken into account, as well as any changes in the IAIG's structure and/or business strategy, and necessary modifications and improvements are identified and made in a timely manner.

CF8.1c.1 The IAIG should assess whether a change occurring in one or more entities may affect the IAIG's risk profile overall. While such a change may impact only locally or within the region initially, the impact on a group-wide basis may not be immediately apparent.

CF8.1c.2 The IAIG's risk management system should take account of all material changes at an entity level that may have an impact on how the IAIG measures and mitigates risk at a group level.

CF 8.1d4c The group-wide supervisor requires the Head of the IAIG to have in place processes and procedures for promoting an appropriate risk culture.

CF8.1d.1 Processes and procedures for promoting an appropriate risk culture should include risk management training, address the issue of independence and create appropriate incentives for staff.

CF8.1d.2 The IAIG's risk culture should support open communication of emerging risks that may be significant to the IAIG and its entities.

8.1.18 As part of its responsiveness to changes in the insurer's risk profile, the risk management system should incorporate a feedback loop based on appropriate information, management processes and objective assessment. The feedback loop provides a process of assessing the effect of changes in risk leading to changes in risk management policy, risk limits and risk mitigating actions. This should ensure that decisions made by the Board and Senior Management are implemented and their effects monitored and reported in a timely and sufficiently frequent manner.

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

8.2 The supervisor requires the insurer to establish, and operate within, an effective and appropriately documented system of internal controls.

[...]

CF8.2a The group-wide supervisor requires the Head of the IAIG to ensure that the internal controls system at the group-wide level ~~is appropriately documented and~~ covers at a minimum the:

- diversity of the activities of the IAIG, including geographical reach of the activities of legal entities within the IAIG;
- intra-group transactions;
- interconnectedness of the legal entities within the IAIG; and
- laws and regulations of the jurisdictions where the IAIG operates.

[...]

Actuarial function

8.6 The supervisor requires the insurer to have an effective actuarial function capable of evaluating and providing advice regarding, at a minimum, technical

provisions, premium and pricing activities, capital adequacy, reinsurance and compliance with related statutory and regulatory requirements.

[...]

CF8.6a The group-wide supervisor requires the Head of the IAIG to ensure that the IAIG actuarial function provides an overview of the IAIG's actuarial activities, functions and risks arising within or emanating from insurance legal entities within the IAIG. This overview includes, at a minimum:

- group-wide risk assessment and management policies and controls relevant to govern the activities of the IAIG's actuarial function ~~matters~~ or ~~the financial condition of the IAIG~~;
- procedures to identify compliance issues at one of the insurance legal entities in the IAIG or the IAIG as a whole, as applicable;
- the IAIG's solvency position, including a calculation of regulatory capital requirements and technical provisions;
- the IAIG's prospective solvency position by conducting capital adequacy assessments and stress tests, under various scenarios, and measuring their relative impact on assets, liabilities, and actual and future capital levels;
- development, pricing and assessment of the adequacy of the IAIG's reinsurance arrangements; and
- actuarial-related risk modelling in the IAIG's Own Risk and Solvency Assessment (ORSA) and use of internal models.

CF8.6b The group-wide supervisor requires the IAIG actuarial function to:

- work with the actuarial functions at the insurance legal entity level to review actuarial information; and
- provide independent advice and reporting to the IAIG Board on the insurance activities and risks posed to the IAIG.

[...]