Guidance Paper No. 2.2.5

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

GUIDANCE PAPER ON ENTERPRISE RISK MANAGEMENT FOR CAPITAL ADEQUACY AND SOLVENCY PURPOSES

OCTOBER 2008

This document was prepared by the Solvency and Actuarial Issues Subcommittee in consultation with IAIS members and observers.

This publication is available on the IAIS website (www.iaisweb.org).

Guidance paper on enterprise risk management for capital adequacy and solvency purposes

Contents

1. Introduction

1. Since its inception in 1994, the IAIS has developed a number of principles, standards and guidance papers to help promote the development, globally, of well-regulated insurance markets. Central to this objective is the development of a common framework for insurance supervision that establishes a common structure within which standards and guidance on insurance solvency assessment may be developed. Insurer solvency takes a central position in risk management by insurers and in insurance supervision. Consideration of the standards and guidance that should apply to enterprise risk management for capital adequacy and solvency purposes, therefore, contributes towards the development of the IAIS framework for insurance supervision.

2. The IAIS recognises that the use of good risk management practices and procedures is an important aspect for insurers in their effective management of the insurance business.

3. Regulatory requirements as described in the Governance Block contained in the Framework paper[1] refer to:

> "governance processes and controls in areas such as the Board, directors, senior management and other organisational aspects, fit and proper testing of directors and management; administrative, organisation and internal controls, including risk management; compliance with legislative requirements; shareholder relationships; and the governance risks posed by group structures".

Supervisory regimes should require insurers to have and maintain corporate governance policies, practices and structures and undertake sound risk management in relation to all aspects of their business. Sound governance is a pre-requisite for a solvency regime to operate effectively.

[1] IAIS *A new framework for insurance supervision: towards a common structure and common standards for the assessment of insurer solvency* (Oct 2005)

4. This paper provides guidance on the establishment and ongoing operation of an enterprise risk management framework, and its importance from a supervisory perspective in underpinning robust solvency assessment. It provides supporting information on the 19 key requirements set out in the *Standard on enterprise risk management for capital adequacy and solvency purposes*. As well as supporting effective solvency assessment, considering the guidance in this paper should assist an insurer to have appropriate risk and capital management policies, practices and structures in place which are applied consistently across its organisation, and embedded within its processes. By encouraging insurers to follow the requirements in the Standard and to consider the supporting guidance in this paper, supervisors will help to maintain the effectiveness of the solvency regime and, in addition, assist in establishing and maintaining a well regulated insurance industry overall.

5. This paper focuses specifically on the risk management element of governance in the context of solvency assessment and capital adequacy. While the paper identifies the broader aspects of risk management to put risk management for capital adequacy and solvency purposes into context, it does not cover these broader aspects in depth. The broader issues of governance are the subject of other IAIS work[2].

1.1 Enterprise Risk Management

6. The raison d'être of insurance is the assumption, pooling and spreading of risk so as to mitigate the risk of adverse financial consequences to individuals and businesses that are policyholders. For this reason, a thorough understanding of risk types, their characteristics and interdependencies, the sources of the risks and their potential impact on the business is essential for insurers. Supervisors should, therefore, seek to ensure that the insurer has a competent understanding of risk and implements sound risk management practices. The ultimate aim of insurance is to create and protect value for policyholders while using capital resources efficiently. A purpose of both risk and capital management is to protect policyholders and capital providers from adverse events. It is therefore natural for insurers to combine the management of risk and capital.

7. There are a number of commonly used terms to describe the process of identifying, assessing, measuring, monitoring, controlling and mitigating risks. This paper uses the generic term enterprise risk management (ERM) in describing these activities in respect of the insurance enterprise as a whole.

8. ERM involves the self-assessment of all reasonably foreseeable and relevant material risks that an insurer faces and their interrelationships. One result, which is particularly relevant for this paper, is that decisions regarding risk management and capital allocation can be co-ordinated for maximum financial efficiency and, from a supervisory viewpoint, the adequate protection of policyholders. A fundamental aspect of ERM is a primary focus on the actions that an insurer takes to manage its risks on an ongoing basis, and specific aspects of those risks, so as to ensure that they are the risks it intends to retain both individually and in aggregate. ERM also involves the rigorous enforcement of risk standards, policies and limits.

9. ERM is an acknowledged practice and is now becoming an established discipline and separately identified function assuming a much greater role in many insurers' everyday business practices. Originally, risk management only facilitated the identification of risks, and was not fully developed to provide satisfactory methods for measuring and managing risks, or for determining related capital requirements to cover those risks. ERM processes being developed today by insurers increasingly use internal models and sophisticated risk metrics to translate risk identification into management

[2] The IAIS will advance further work on governance issues through the Governance and Compliance Subcommittee.

actions and capital needs. Such an approach typically adopts a total balance sheet approach whereby the impact of the totality of material risks is fully recognised on an economic basis. A total balance sheet approach reflects the interdependence between assets, liabilities, capital requirements and capital resources, and identifies a capital allocation, where needed, to protect the insurer and its policyholders and to optimise returns to the insurer on its capital[3].

10. ERM provides a link between the ongoing operational management of risk and longer-term business goals and strategies. Appropriate risk management policies should be set by each insurer according to the nature, scale[4] and complexity of its business. The guidance in this paper focuses on the link between risk management and the management of capital adequacy and solvency.

11. The IAIS *Standard on asset-liability management (Oct 2006)* identifies asset-liability management as a vital element within an ERM framework. Asset-liability management (ALM) is the practice of managing a business so that decisions and actions taken with respect to assets and liabilities are coordinated. As ERM includes ALM, this ERM guidance paper addresses the solvency and capital adequacy aspects of ALM as well.

12. The IAIS recognises the different levels of sophistication of supervisors and insurance markets around the world and acknowledges that the guidance within this paper may not be fully achievable by some insurers and in some markets in the near future. Nevertheless, the IAIS believes that good risk management practices and procedures need to be in place for a solvency regime to be effective. ERM that follows the guidance in this paper is expected to enhance confidence in assessing an insurer's financial strength. The IAIS envisages that solvency regimes will, over time, be developed towards conformity with the IAIS standards and guidance papers. The IAIS nevertheless wishes to emphasise that this paper does not prescribe a specific aspect of a solvency regime which is to be applied compulsorily by IAIS members. It should be noted in this respect that the concepts presented and the terminology used in IAIS papers are intended to be of a general nature and should not be interpreted as legally binding in a specific supervisory regime.

13. This paper focuses on an insurer as a single entity and risk management as it relates to its solvency assessment. It is recognised that risk management may be conducted at a group level and that risk management by the insurer may only be part of a broader system. The issues surrounding insurance groups and their supervision are not within the scope of this paper and are the subject of separate IAIS work[5].

---

3 Refer to the IAIS *Standard and Guidance paper on the structure of regulatory capital requirements* (Oct 2008) for more detail on capital requirements.

4 The scale of the business is a relevant factor. Some insurers may be less well diversified and more susceptible to risks arising from external sources. They may also need to structure their risk management functions differently from other insurers and commission external consultants to achieve satisfactory standards and robust processes; they may need to use reinsurance to a greater extent.

5 The IAIS Insurance Groups and Cross-sectoral Issues Subcommittee (IGSC) will advance further work on group-wide supervision. The IAIS IGSC and the Solvency and Actuarial Issues Subcommittee are also developing a joint Issues paper on group-wide solvency assessment.

2. Governance and an Enterprise Risk Management framework

Requirement 1

As part of its overall governance structure, an insurer should establish, and operate within, a sound ERM framework which is appropriate to the nature, scale and complexity of its business and risks.

Requirement 2

The ERM framework should be integrated with the insurer's business operations and culture, and address all reasonably foreseeable and relevant material risks faced by the insurer in accordance with a properly constructed risk management policy.

Requirement 3

The establishment and operation of the ERM framework should be led and overseen by the insurer's board and senior management.

Requirement 4

For it to be adequate for capital management and solvency purposes, the framework should include provision for the quantification of risk for a sufficiently wide range of outcomes using appropriate techniques.

Requirement 5

Measurement of risk should be supported by accurate documentation providing appropriately detailed descriptions and explanations of risks.

14. Since risk-taking is the fundamental element of an insurer's business, the supervisor should encourage an insurer to establish an adequate ERM framework, appropriate to the nature, scale and complexity of its business and risks, for evaluating and managing the risks for its businesses as a whole. In doing so the insurer should take into account the different characteristics of individual business units, developing the tools to operate the framework in practice and to monitor its effectiveness. The insurer would be expected to tailor its enterprise risk management framework to its risk profile, strategy and organisation. The supervisor should also encourage the insurer to have clear policies and procedures to recognise, analyse, assess, measure, and manage risks, including defining quantitative and/or qualitative limits on the amount of different types of risk, taking into account the capital available and the appropriate risk mitigating tools employed (e.g. reinsurance, hedging etc). Such policies and processes for the management of risk are an integral part of the insurer's ERM framework and should be established and approved, regularly monitored and reviewed by the board and senior management[6].

[6] The IAIS *Insurance core principles and methodology* (2003) (ICPs), ICP 9 and 19.

2.1 Governance and risk management

15. The governance of an insurer often influences its corporate culture and risk tolerance. Governance is therefore important in ensuring that the development of an insurer's ERM framework is integrated with the desired business culture and is consistent with the behaviour expected of the insurer's staff. The supervisor should require an insurer to have in place internal processes and controls that are adequate for and appropriate to the nature, scale and complexity of the business, as it is the oversight and reporting systems that allow the board and management to monitor and control the operations[7]. An insurer's ERM framework is part of these internal processes and controls and should be integrated with the insurer's business operations. Supervisors should note that the appropriate ERM framework is heavily dependent on the nature, scale and complexity of the risks of the insurer. The approach should be proportionate and fit-for-purpose. A 'one-size-fits-all' approach should therefore be avoided.

16. Although risk management practices and procedures should be embedded throughout the hierarchy of an insurer, the responsibility for effective enterprise risk management policies and processes ultimately lies with the board and senior management. An insurer's risk management should incorporate both 'top-down' and 'bottom-up' approaches. The board and senior management should take the lead in developing and implementing risk management policy so that the insurer meets its strategic goals. The board and senior management should ensure that significant new activities of the insurer (including the creation of a new type of exposure) are approved at an appropriate level of authority.

17. The board and senior management are responsible for establishing and maintaining a proportionate and effective internal control system. Furthermore, they should provide suitable oversight of the risk management system that includes setting and monitoring policies so that all reasonably foreseeable and relevant material risks are identified, assessed, reported, monitored and controlled on an ongoing basis. Responsibility for risk management entails periodic review of the procedures and processes used including significant changes to those processes and assurance that internal controls are in place in relation to those processes. The board and senior management should also understand the limitations of the risk management framework and the potential impact in practice of these limitations on risk management, and where significant, should ensure that the framework is modified accordingly. Reports on the risk exposure of the insurer should be regularly provided to and reviewed by the board and senior management using appropriate oversight committees, if established, such as a Board Audit Committee or Board Risk Committee.

18. 'Bottom-up' processes should also be in place to ensure that the insurer's risk culture adequately supports realistic risk reporting rather than excessively optimistic, slow or inappropriately filtered reporting of risk issues. A bottom-up approach enables specific risks to be monitored and managed at a business or activity level within risk limits that are consistent with the overall risk tolerance of the insurer. The insurer should also have in place an appropriate escalation process for risk reporting, particularly for dealing with risk issues that emerge outside formal reporting cycles.

19. Responsibility for risk management should be clearly allocated. This may include the appointment of a sufficiently resourced risk management function with responsibility for the design and implementation of the ERM framework, where appropriate and proportionate. Employees should have a clear understanding of their role in risk management, and it is the responsibility of senior management and delegated risk management authorities to ensure this. An insurer should have appropriate resources so that monitoring systems are able to evolve with its business risks and are able to meet the increasing sophistication of ERM requirements and practices.

---

[7] The IAIS *Insurance core principles and methodology* (2003) (ICPs), ICP 10.

20. An insurer's ERM framework should seek to avoid conflicts of interest in the insurer's functions and ensure that any conflicts that remain can be and are effectively managed. For example, the role of a risk management function referred to above, where established, would be expected to be independent of business line management. The framework for internal controls within the insurer should include arrangements for delegating authority, and the proper segregation of duties including, in particular, a separation of the management of risks from the assessment of the effectiveness of risk management. This assessment should be undertaken by a suitably qualified internal or external independent party. In principle, from a governance perspective, those responsible for the design of the ERM framework should be independent of those assessing its effectiveness. An independent review by external consultants should be considered, where proportionate to the scale of business, if the insurer does not have a qualified internal audit function that can perform this type of assessment. Where a full segregation would not be practical, the insurer should take other appropriate measures (which could be internal or external to the insurer) to ensure that a conflict of interest is effectively managed. The internal controls should address checks and balances, for example, cross-checking, dual control of assets, double signatures etc[8] [9].

21. An insurer should maintain an audit trail of changes in its risk management framework to help ensure that the framework remains broadly consistent over time and that any changes are fully explained. The existence of the audit trail would be expected to provide the supervisor with confidence that the framework is being effectively managed.

22. Where an insurer outsources some of its functions, its risk management framework should encompass these functions to provide proper oversight. Prior to outsourcing, an insurer should have in place a comprehensive policy, based on a risk analysis, to guide the assessment of whether and how activities can be appropriately outsourced, and how those outsourcing arrangements can be changed or terminated. Risk concentrations, limits on the acceptable overall level of outsourced activities and risks arising from outsourcing multiple activities to the same service provider should all be considered. An insurer should ensure that outsourcing arrangements neither diminish its ability to fulfil its obligations to policyholders and supervisors, nor impede effective supervision. The board retains responsibility for the outsourcing policy and related overall responsibility for activities undertaken under that policy.

23. Outsourcing relationships should be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties. An appropriate governance structure with clearly defined roles and responsibilities on the part of the outsourcer should exist throughout the engagement process and contract term. A comprehensive outsourcing risk management programme should provide for an ongoing monitoring and controlling of all relevant aspects of outsourcing arrangements and for procedures guiding corrective actions to be taken when certain events occur.

Risk identification

24. The ERM framework should identify and address all reasonably foreseeable and relevant material risks to which an insurer is, or is likely to become, exposed. Such risks should include, at a minimum, underwriting risk, market risk, credit risk, operational risk and liquidity risk.

25. After identification of relevant risks, an insurer should highlight significant and material risks together with possible key leading indicators (e.g. a relevant stock market

[8] Refer to ICP 9, essential criterion b.
[9] Refer to ICP 10, essential criterion b.

indicator). This information should be included in regular management information which is relevant and focussed.

Causes of risk and the relationship between risks

26. An insurer should consider the causes of different risks and their impacts and assess the relationship between risk exposures. By doing so, an insurer can better identify both strengths and weaknesses in governance, business and control functions, and should use and improve risk management policies, techniques and practices and change its organisational structure to make these improvements where necessary. The insurer should also assess external risk factors which, if they were to crystallise, could pose a significant threat to its business. The insurer should recognise the limitations of the methods it uses to manage risks, the potential impact these limitations may have, and adapt its risk management appropriately.

Analysing and modelling the level of risk

27. The level of risk is a combination of the impact that the risk will have on the insurer and the probability of that risk materialising. Risks should be modelled to assess their effect on an insurer's business. Different modelling approaches[10] may be appropriate depending on the nature, scale and complexity of a risk and the availability of reliable data on the behaviour of that risk. For example, a low frequency but high impact risk where there is limited data, such as catastrophe risk, may require a different approach from a high frequency, low impact risk for which there is substantial amounts of experience data available.

28. Stress and scenario analysis[11] can be used (as a measuring tool) by insurers to analyse the impact of events, such as catastrophes. It can also be used in developing long-term business plans, by modelling the impact of changes on the level of risk to which the insurer is exposed and its implications for risk management.

29. An insurer should regularly produce quantitative assessments of the risks its business faces as this provides it with a disciplined method of monitoring risk exposure. Assessments undertaken at different times should be produced on a broadly consistent basis overall, so that any variations in results can be readily explained. Such analysis also aids an insurer in prioritising its risk management. Internal models can play an important role in facilitating this process[12] and supervisors should expect larger and/or more complex insurers to make use of such models, where appropriate, for parts or all of their business.

30. Where internal models are relied on, it must be remembered that, regardless of how sophisticated the model may be, it cannot exactly replicate the real world. As such, the use of models itself generates risk (modelling and parameter risk) which, if not explicitly quantified, at least needs to be acknowledged and understood as the insurer implements its ERM framework.

31. Where a risk is not readily quantifiable, for instance some operational risks and reputational risks, an insurer should make a qualitative assessment that is appropriate to that risk and sufficiently detailed to be useful for risk management. An insurer should analyse the controls needed to manage such risks to ensure that its risk assessments are reliable and consider events that may result in high operational costs or operational

---

10 'Modelling' in this context does not necessarily mean complex stochastic modelling, it can also include less sophisticated methods.

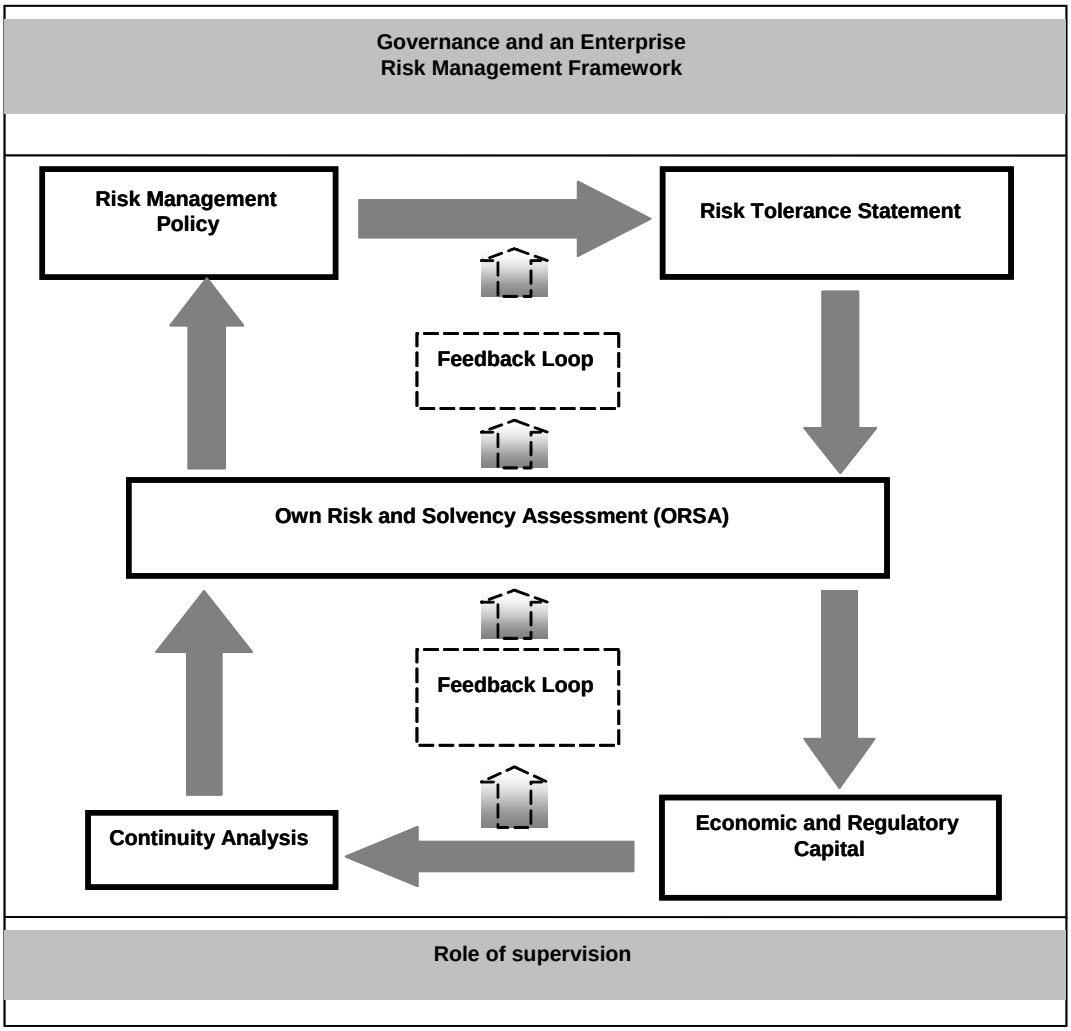
11 Refer to the IAIS *Guidance Paper on stress testing by insurers* (Oct 2003)

12 Internal models are discussed further in the IAIS *Standard and Guidance paper on the use of internal models for regulatory capital purposes* (Oct 2008).

failure. Such analysis is expected to inform an insurer's judgements in assessing the size of the risks as well as enhance overall risk management.

32. Measurement of risk should be supported by accurate documentation providing appropriately detailed descriptions and explanations of risks.

33. The following diagram illustrates a best practice ERM framework showing the key features of the framework as described in the following sections of this paper.



2.2 Risk management policy

Requirement 6

An insurer should have a risk management policy which outlines the way in which the insurer manages each relevant and material category of risk, both strategically and operationally.

Requirement 7

The policy should describe the linkage with the insurer's tolerance limits, regulatory capital requirements, economic capital and the processes and methods for monitoring risk.

34. As part of its ERM framework, an insurer should describe its policy for controlling and mitigating the risks it is exposed to and the processes and methods for monitoring risk. A risk management policy would be expected to include a description of the insurer's policies towards reinsurance, diversification/specialisation, the use of financial instruments such as derivatives, and other aspects of asset-liability management.

35. An insurer's risk management policy should describe how its risk management links with its management of capital (regulatory capital requirement and economic capital). For the purposes of this paper, the term "economic capital" refers to the capital needed by the insurer to satisfy its risk tolerance and support its business plans which is determined from an economic assessment of the insurer's risks, the relationship between them and the risk mitigation in place. This does not necessarily require the use of an economic capital model but implies the use of techniques that are proportionate to the nature, scale and complexity of an insurer's business.

36. As an integral part of its risk management policy, an insurer should also describe how its risk management links with corporate objectives, strategy and current circumstances. A reasonably long time horizon, consistent with the nature of the insurer's risks and the business planning horizon, should be considered by the risk management policy so that it maintains relevance to the insurer's business going forward. This can be done by using methods, such as scenario models, that produce a range of outcomes based on plausible future business assumptions. The insurer should monitor risks so that the board and senior management are fully aware of how the insurer's risk profile is changing. Where models are used for business forecasting insurers should perform back-testing, to the extent practicable, to validate the accuracy of the model over time.

2.3 Risk tolerance[13] statement

Requirement 8

An insurer should establish and maintain a risk tolerance statement which sets out its overall quantitative and qualitative tolerance levels and defines tolerance limits for each relevant and material category of risk, taking into account the relationships between these risk categories.

Requirement 9

The risk tolerance levels should be based on the insurer's strategy and be actively applied within its ERM framework and risk management policy.

Requirement 10

The defined risk tolerance limits should be embedded in the insurer's ongoing operations via its risk management policies and procedures.

37. After an insurer has developed its risk management policy, established appropriate tools for analysing, assessing, monitoring and measuring risks and identified its risk exposures, an insurer would be expected to establish and maintain a risk tolerance statement. An insurer's overall risk tolerance statement should set out the level of risk to which it is willing and able to be exposed, taking into account its financial strength and the nature, scale and complexity of its business risks, the liquidity and

[13] In this paper, the term 'risk tolerance' is used to include the active retention of risk that is appropriate for an insurer in the context of its strategy, financial strength, and the nature, scale and complexity of its business risks. The concepts of risk tolerance, in the particular context of ALM, are also discussed in the IAIS *Standard on asset-liability management* (Oct 2006).

transferability of its business, and the physical resources it needs to adequately manage its risks.

38. The risk tolerance statement should define the insurer's 'tolerance limits' which give clear guidance to operational management on the level of risk to which the insurer is prepared to be exposed and the limits of risk to which they are able to expose the insurer as part of their work. An insurer should consider how these tolerance limits are to be suitably embedded in its ongoing operational processes. This can be achieved, for instance, by expressing tolerance limits in a way that can be measured and monitored as part of ongoing operations. Stress testing can also provide an insurer with a tool to help ascertain whether its tolerance limits remain suitable for its business.

2.4 Risk responsiveness and feedback loop

Requirement 11

The insurer's ERM framework should be responsive to change.

Requirement 12

The ERM framework should incorporate a feedback loop, based on appropriate and good quality information, management processes and objective assessment, which enables the insurer to take the necessary action in a timely manner in response to changes in its risk profile.

39. The ERM framework and risk management policy of the insurer should be responsive to change as a result of both internal and external events. The framework should include mechanisms to incorporate new risks and new information on a regular basis. For example, new risks identified from within the business may include new acquisitions, investment positions, or business lines. New information may become available from external sources, as a result of evolution of the environment affecting the nature and size of underlying risks. Supervisory and legislative requirements, rating agency concerns (if applicable), political changes, major catastrophes or market turbulence may all make changes necessary. The framework and policy should also be responsive to the changing interests and reasonable expectations of policyholders and other stakeholders.

40. Within the ERM framework there should also be a 'feedback loop'. This should ensure that decisions made by the board and senior management are implemented and their effect monitored and reported in a timely and sufficiently frequent manner via good management information. The feedback loop is the process of assessing the effect, within the ERM framework, of changes in risk leading to changes in risk management policy, tolerance limits and risk mitigating actions. Without this continual updating process, complemented by special one-off changes in response to major events, the ERM framework would not remain relevant in assisting the insurer in meeting its strategic and risk objectives. In this context, the existence of good governance processes and practices is crucial to the effective operation of the ERM framework (refer to section 2.1).

3. Own Risk and Solvency Assessment (ORSA)

Requirement 13

An insurer should regularly perform its own risk and solvency assessment (ORSA) to provide the board and senior management with an assessment of the adequacy of its risk management and current, and likely future, solvency position.

Requirement 14

The ORSA should encompass all reasonably foreseeable and relevant material risks including, as a minimum, underwriting, credit, market, operational and liquidity risks. The assessment should identify the relationship between risk management and the level and quality of financial resources needed and available.

41. The ability of an insurer to reflect risks in a robust manner in its own assessment of risk and solvency is supported by an effective overall ERM framework, and by embedding its risk management policy in its operations. Regardless of the nature, scale or complexity of its business and irrespective of the approach used by an insurer to manage risk and capital, every insurer should undertake its own risk and solvency assessment (ORSA) and document the rationale, calculations and action plans arising from this assessment. It is recognised that the nature of the assessment undertaken by a particular insurer should be appropriate to the nature, scale and complexity of its risks.

42. In its ORSA an insurer should consider all material risks that may have an impact on its ability to meet its obligations to policyholders, including in that assessment a consideration of the impact of future changes in economic conditions or other external factors. An insurer should undertake an ORSA on a regular basis so that it continues to provide relevant information for its management and decision making processes. The insurer should regularly reassess the causes of risk, and the extent to which particular risks are material. Significant changes in the risk profile of the insurer should prompt it to undertake a new ORSA. Risk assessment should be done in conjunction with consideration of the effectiveness of applicable controls to mitigate the risks.

43. While the prime purpose of the ORSA is to provide the board and senior management with an assessment of whether its risk management and solvency position is currently adequate and is likely to remain so in future, the output of an insurer's ORSA may also serve an important role in the supervisory review process - as a supervisory tool, informing the supervisor's understanding of the risk exposure and solvency position of the insurer.

3.1 Economic and regulatory capital

Requirement 15

As part of its ORSA an insurer should determine the overall financial resources it needs to manage its business given its own risk tolerance and business plans, and to demonstrate that supervisory requirements are met.

Requirement 16

The insurer's risk management actions should be based on consideration of its economic capital, regulatory capital requirements and financial resources.

44. In the context of its overall ERM framework, an insurer should perform its ORSA and have risk and capital management processes in place to monitor the level of its financial resources relative to its economic capital and the regulatory capital requirements set by the solvency regime.

45. In the context of its own assessment, an insurer should clearly distinguish between current capital needs and its projected future financial position, having regard for its longer-term business strategy and, in particular, new business plans.

46. While holding capital to cover risk is not necessarily the most effective way of managing it, it is important that an insurer has regard for how risk management and capital management relate to and interact with each other. Therefore, an insurer should determine the overall financial resources it needs, taking into account its risk tolerance and business plans, based on an assessment of its risks, the relationship between them and the risk mitigation in place. Determining economic capital helps an insurer to assess how best to optimise its capital base, whether to retain or transfer risk, and how to allow for risks in its pricing. It also helps to give the supervisor confidence that risks are being well managed.

47. Although the amounts of economic capital and regulatory capital requirements and the methods used to determine them may differ, an insurer should be aware of, and be able to analyse and explain, these differences. Such analysis helps to embed supervisory requirements into an insurer's ORSA and risk and capital management, so as to ensure that obligations to policyholders continue to be met as they fall due.

3.2 Using an internal model for the ORSA

48. An insurer may consider that the assessment of current financial resources and the calculation of regulatory capital requirements would be better achieved through the use of internal models. More information on the use of internal models in meeting regulatory capital requirements and the supervisory approval required can be found in the IAIS Standard and Guidance paper on the use of internal models for regulatory capital purposes.

49. Where an internal model is used for the ORSA, it is likely to be an important strategic and operational decision-making tool and be most useful if it enables the insurer to integrate its risk and capital management processes; that is, assisting with both the assessment of the risks faced within its business and the determination of the economic capital needed, where appropriate, to meet those risks.

50. As identified in paragraph 24, an ERM framework should reflect all reasonably foreseeable and relevant material risks that affect the insurer’s business. To be most effective, therefore, an internal model used for the ORSA needs to address all those identified risks and assess their impact on the insurer’s business given the possible situations that could occur. The risks to be considered should include underwriting risk, credit risk, market risk, operational risk and liquidity risk (including any significant risk concentrations). The categories of risks considered should be clearly defined. The methods by which this analysis could be conducted range from simple stress testing of events to more complex interlocking stochastic modelling as appropriate to the nature, scale and complexity of the risks concerned[14].

51. When used for the ORSA, the insurer’s internal model is likely to be calibrated on the basis of defined modelling criteria which the insurer believes will determine the level of capital appropriate and sufficient to meet its business plan and strategic objectives. These modelling criteria are likely to include the basis for valuation of the assets and liabilities, and the confidence level, risk measure, and time horizon which the insurer

[14] See IAIS *Guidance paper on stress testing by insurers* (Oct 2003).

considers appropriate to its risk tolerance and business plans. An insurer is likely to consider various factors in order to determine the modelling criteria used to determine its economic capital; for example choosing a level to achieve a certain investment rating, or to meet other business objectives.

52. In constructing its internal model for the ORSA, an insurer is likely to adopt risk modelling techniques and approaches appropriate to the nature, scale and complexity of the risks incorporated within its risk strategy and business objectives. An insurer may consider various inputs to the modelling process, such as economic scenarios, asset portfolios and liabilities from in-force or past business[15]. It is likely that the modelling criteria and the various inputs to the modelling would be established in the context of the insurer continuing to operate on a going concern basis (unless the insurer is in financial difficulty).

53. An internal model used in the ORSA to determine the economic capital enables the insurer to allocate sufficient financial resources to ensure it can continue to meet its policyholder liabilities as they fall due, at a confidence level appropriate to its business objectives. To fully assess policyholder liabilities in this way, all liabilities that need to be met to avoid putting policyholder interests at risk need to be considered, including any liabilities for which a default in payment could trigger the winding up of the insurer.

54. An internal model used by an insurer in the context of its ORSA for determining its own economic capital needs should not need supervisory approval for that purpose. However, an insurer would be expected to review its own internal model and validate it so as to satisfy itself of the appropriateness of the model for use as part of its risk and capital management processes[16]. It would be expected to calibrate the model according to its own modelling criteria. As well as internal review, the insurer may wish to consider an external review of its internal model by appropriate specialists.

55. As noted in paragraph 43, the output of an insurer's ORSA may also serve an important role in the supervisory review process. This is similarly the case where an internal model is used in the context of an insurer's ORSA. In these circumstances, the supervisor may consider the insurer's internal model, its inputs and outputs and the validation processes, as a source of insight into the risk exposure and solvency position of the insurer.

---

15 The methodology should allow for any regulatory constraints on the application and transfer of assets, e.g. in jurisdictions where insurers are required to segregate the assets backing the liabilities of different classes of insurance into separate funds and where the transfer of assets between funds is restricted by regulations.

16 Validation should be carried out by a different department or personnel to those that created the internal model to facilitate independence.

3.3 Continuity analysis

Requirement 17

As part of its ORSA, an insurer should analyse its ability to continue in business, and the risk management and financial resources required to do so over a longer time horizon than typically used to determine regulatory capital requirements.

Requirement 18

Such continuity analysis should address a combination of quantitative and qualitative elements in the medium and longer-term business strategy of the insurer and include projections of the insurer's future financial position and analysis of the insurer's ability to meet future regulatory capital requirements.

56. An insurer should be able to demonstrate an ability to manage its risk over the longer term under a range of plausible adverse scenarios. An insurer's capital management plans and capital projections are therefore key to its overall risk management strategy. These should allow the insurer to determine how it could respond to unexpected changes in markets and economic conditions, innovations in the industry and other factors such as demographic, legal and regulatory, medical and social developments. Supervisors may require an insurer to undertake periodic, forward-looking continuity analysis and modelling of its ability to meet its regulatory capital requirements under various conditions.

57. A clear distinction should be made between the assessment of current capital requirements and the projections, stress testing and scenario analyses used to assess an insurer's financial condition for the purposes of strategic risk management including maintaining solvency.[17] Continuity analysis is the process of ensuring sound, effective, and complete processes, strategies and systems. It helps to assess and maintain on an ongoing basis the amounts, types and distribution of financial resources needed to cover the nature and level of the risks to which an insurer is or might be exposed and to enable the insurer to identify and manage all reasonably foreseeable and relevant material risks. In doing so, the insurer assesses the impact of possible changes in business or risk strategy on the level of economic capital needed as well as the level of regulatory capital requirements.

58. Such continuity analysis should have a time horizon needed for effective business planning, for example 3 to 5 years, which is longer than typically used to determine regulatory capital requirements[18]. It should also place greater emphasis than may be considered in regulatory requirements on new business plans and product design and pricing, including embedded guarantees and options, and the assumptions appropriate given the way in which products are sold. In order for continuity analysis to remain most meaningful, an insurer should also consider changes in external factors such as possible future events including changes in the political or economic situation.

59. Through the use of continuity analysis an insurer is better able to link its present capital requirements with future business plan projections, and so better ensure its ability to continue to meet capital requirements in the future. In this way the insurer further embeds its enterprise risk management into its ongoing and future operations.

---

17 The scenarios used for such assessments may be determined by the insurer or the supervisor. Refer to the IAIS *Guidance paper on stress testing by insurers* (Oct 2003).

18 The comparison with the time horizon for determining regulatory capital requirements is with the defined time horizon over which the level of safety is specified or 'shock period' as described in the IAIS *Standard and Guidance paper on the structure of regulatory capital requirements* (Oct 2008).

60. An internal model may also be used for the continuity analysis allowing the insurer to assess the capital consequences of strategic business decisions in respect of its risk profile. For example, the insurer may decide to reduce its exposure to certain risks by writing different types of business, in order to reduce the capital that is needed to be held against such risks, potentially freeing up resources for use elsewhere. This process of capital management enables the insurer to change its capital exposure as part of its long-term strategic decision making.

61. As a result of such strategic changes, the risk profile of an insurer may alter, so that different risks need to be assessed and quantified within its internal model. In this way, an internal model may sit within a cycle of strategic risk and capital management, and provides the link between these two processes.

4. Role of supervision in risk management

Requirement 19

The supervisor should undertake reviews of an insurer's risk management processes and its financial condition. The supervisor should use its powers to require strengthening of the insurer's risk management, including solvency assessment and capital management processes, where necessary.

62. The insurer's ERM framework and risk management processes (including internal controls) are critical to solvency assessment and capital management. Supervisors should therefore assess the adequacy and soundness of the insurer's framework and processes. However, company operations are primarily the responsibility of the board and senior management and the board and management need to be able to exercise their own discretion or business judgment to carry out these responsibilities.

63. Supervisors should review an insurer's internal controls and monitor its capital adequacy, requiring strengthening of these controls where necessary. Where internal models are used to calculate the regulatory capital requirements particularly close interaction between the supervisor and insurer is important.

64. Supervisors should suitably monitor the techniques employed by the insurer for risk management and capital assessment, and intervene where weaknesses are identified. Supervisors should not take a 'one-size-fits-all' approach to insurers' risk management but base their expectations on the complexity of an insurer's risks and the nature, scale and complexity of its business. In order to do this, supervisors need to ensure they have sufficient and appropriate resources and capabilities. Supervisors may, for instance, have a risk assessment model or programme in which they can assess their insurers' overall condition (e.g. risk management, capital adequacy and solvency position) and ascertain the likelihood of insurers breaching their regulatory requirements. Supervisors may also prescribe minimum aspects that an ERM framework should address.

65. Supervisors should require appropriate information on risk management and risk and solvency assessments from each insurer they regulate. This not only provides supervisors with a long-term assessment of capital adequacy to aid in their assessment of insurers, but encourages insurers to use risk management effectively. This could also be achieved by, for instance, a supervisor requiring or encouraging insurers to provide a solvency and financial condition report. Such a report could include a description of the relevant material categories of risk that the insurer faces, its overall financial resource needs including its economic capital and regulatory capital requirements as well as the available capital to meet these requirements, and projections of how such factors will

develop in future. Where, after appropriate request from the supervisor, an insurer fails to report adequate information about its risk and capital management practices, processes and procedures from which the supervisor can monitor the insurer, the supervisor should intervene or apply penalties appropriately. In addition, an insurer should have a duty to report to the supervisor a breach in regulatory requirements as soon as it occurs.

66. Publicly disclosing information on risk management should work towards the IAIS's objective of improving the transparency and comparability of existing solvency regimes. The IAIS supports the need for balance regarding the level of information to disclose about an insurer's risk management whilst producing sufficient information for external and internal stakeholders which is useful and meaningful. Therefore, the IAIS recognises that the requirements for public disclosure of information on risk management, including possible disclosure of elements of a solvency and financial condition report, should be carefully considered by supervisors taking into account the proprietary nature of the information, whether it is commercially sensitive and the potential for its publication to have adverse effects on insurers.

67. Where an insurer's risk management practices and processes are not considered adequate by the supervisor, the supervisor should take appropriate action. This could be in the form of further supervisory reporting or additional qualitative and quantitative requirements arising from the supervisor's assessment[19]. However, additional quantitative requirements should only be applied in appropriate circumstances and subject to a transparent framework. If routinely applied, such measures may undermine a consistent application of standardised approaches to regulatory capital requirements.

68. Conversely, an insurer that manages its risks and capital well should be recognised and the level of supervision adapted to be commensurate with a risk-based supervisory approach. This does not necessarily mean a low level of supervision, but a level of supervision appropriate to the level of risk to which the insurer is exposed and its ability to manage the risks. An insurer's effective management of risk and capital does not necessarily mean the use of complex internal models, but a degree of risk management appropriate to the nature, scale and complexity of the insurer. Importantly, risk sensitive regulatory financial requirements should provide the incentive for optimal alignment of risk and capital management by the insurer and regulation.

[19] More information on forms of appropriate supervisory actions can be found in the IAIS *Standard and Guidance paper on the structure of regulatory capital requirements* (Oct 2008).