

# 04

## No surprises: An opportunity to reinforce governance

ÅSA MALMSTRÖM ROGNES, GARVAN O'NEILL AND WENDY REED

Solvency II is set to impose extensive governance requirements for insurers of all sizes. Although some insurers may opt for straight compliance, this may miss a valuable opportunity to strengthen stakeholder confidence and provide greater assurance for the board. Åsa Malmström Rognes, Garvan O'Neill and Wendy Reed look at the competitive benefits of building the latest concepts in risk and compliance management into a tailored framework for governance.



These are nervous times for insurance executives. For an industry already grappling with challenges ranging from climate change to geopolitical instability, the recent shockwaves in the financial markets offer the starkest possible warning of what can happen when risk governance is not up to scratch.

Even before Solvency II comes into force, many insurers are likely to face tougher legislation and heightened regulatory scrutiny in the wake of the financial turmoil. However, far from being simply a regulatory imperative, the ability to effectively identify, measure and manage business and compliance risks now needs to be integral to the way insurers run their companies. One of the most important benefits at any time is greater transparency and comfort for the board and wider senior management ('no surprises'), especially in uncertain and unstable markets.

Solvency II seeks to ensure that insurers are suitably equipped to deal with a rapidly evolving risk landscape by fortifying their Pillar 1 capital reserves with tough governance standards under Pillar 2. Justifying this approach, the European Commission noted that 'poor management and inappropriate risk decisions rather than inadequate capitalisation per se' are the primary causes of insurance company failures.<sup>1</sup> As a result, Solvency II places primary responsibility for risk management and compliance on the board and senior management and requires insurers to demonstrate that both are integral to business decision making. Under Pillar 2, companies will be required to develop a systematic and comprehensive framework

**'Robust governance requirements are a pre-requisite for an efficient solvency system. Some risks may be addressed through governance requirements rather than by setting quantitative requirements'<sup>2</sup>**

From 'EC Explanatory Memorandum on Draft Framework Directive'

of risk control and oversight, founded on the clear definition and allocation of firm-wide governance roles and responsibilities and underpinned by independent actuarial, risk management, compliance and internal audit functions.

In essence, the governance system should ensure that:

- A clear and tangible definition of the risk appetite is in place and consistently communicated and applied throughout the organisation;
- All aspects of business planning and management take relevant risks into account;
- All key personnel meet 'fit and proper' requirements; and
- Management retains oversight of all outsourced activities or functions.

Clearly, the governance provisions of Solvency II, including what for many will be the establishment of new functions and management structures, are likely to prove taxing. There may also be some potential tension between rigorous risk management and an entrepreneurial approach. It is therefore important to ensure an appropriate balance between

controls and business aspirations. This includes building risk considerations into performance objectives and incentives.

### One size does not fit all

The principle of 'proportionality' requires companies to design their governance structures according to the scale, nature and complexity of their specific business. This can mean less onerous demands for

### Solvency II: Governance requirements

Article 41 of the proposed directive requires insurers to put 'in place an effective system of governance which provides for sound and prudent management', including an 'adequate transparent organisational structure with a clear allocation and appropriate segregation of responsibilities'.<sup>3</sup> This system should be in keeping with the nature, scale and complexity of the business and include board-approved written policies on risk management, internal control, internal audit and, where appropriate, outsourcing. It should also be subject to regular reviews.

1 'Solvency II: Frequently Asked Questions', published by the European Commission (EC) on 10.07.07. The view draws on the findings of 'Prudential Supervision of Insurance Undertakings' ('Sharma Report'), a study carried out for the EU Insurance Supervisors Conference, December 2002.

2 'Explanatory Memorandum' published by the European Commission with amended draft framework directive in February 2008.

3 Amended draft framework directive published by the EC in February 2008.

# 04 No surprises: An opportunity to reinforce governance

some. To enable firms to flex their governance framework appropriately, the Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS) envisages that some governance functions may be outsourced or combined within smaller or less risky organisations.<sup>4</sup> This should be good news for many insurers, as our experience indicates that only larger organisations tend to see significant benefits in, for example, separate risk management and compliance functions.

However, proportionality cuts both ways, as size is not the determining factor. Small firms with risky portfolios will face stricter supervisory demands, while larger, less risky, firms and mono-line companies should have lower governance benchmarks to meet. CEIOPS is currently refining its approach to proportionality and we can expect more details in its advice to the European Commission on the Level 2 implementing measures. Firms of all configurations and sizes would be well-advised to provide input into this process.

Solvency II presents insurers with a central challenge in defining and implementing a governance system that appropriately reflects their individual risk profile. The governance structures and procedures need to be based on a regularly reviewed, organisation-specific risk assessment. This should be aligned with the overall strategy and direction of the firm, in order to convince supervisors that governance structures and procedures are fit for purpose. Defining and allocating roles and responsibilities appropriately across functions (including risk management and compliance) requires a sound appreciation of the relative importance of each within a particular organisation. In turn, the suitability and efficiency of the governance framework will

need to be constantly reappraised as part of the Solvency II Own Risk and Solvency Assessment (ORSA). The key challenge is determining an appropriate structure, which is able to adapt smoothly to evolving risks and changing strategic objectives.

## Risk management

In the lead up to Solvency II, further impetus for more effective governance has been coming from the rating agencies, which in recent years have been looking more closely at the quality of insurers' risk management systems as part of their financial strength evaluations. Standard and Poor's believes that 'all insurers, independent of their size and complexity, need to have capabilities to limit their risk exposure and losses to within appropriate tolerances'.<sup>5</sup> In line with Solvency II, the keys to this are ensuring that an appreciation of how to manage risk permeates through the organisation and, building on this understanding, that risk considerations are fully embedded into governance and decision making.

The development of enterprise risk management (ERM) capabilities could help to underpin this more structured approach to governance and related compliance and risk management. However, it is notable that few insurers have earned high marks from the ratings agencies for their ERM. For example, less than 15% of insurers were rated as 'strong' or 'excellent' in the latest Standard and Poor's assessment.<sup>6</sup> Some have even received a rating downgrade as a result.

PricewaterhouseCoopers 2008 study of ERM in the insurance industry further emphasised the need for greater integration between risk and business management, particularly at ground level.<sup>7</sup>

Using Solvency II as an opportunity to strengthen integration across different aspects of risk management and between risk, business and compliance management could therefore help to create a more secure and efficient framework of governance. A foundation for this is a clear understanding of who is responsible for risk management within each link of the decision-making and risk-taking chain. This enables companies to allocate resources more effectively and ensures that risk is evaluated and communicated on a clear, timely and consistent firm-wide basis. In most cases, business units should assume primary responsibility for identifying, monitoring and managing the risks they take (first line of defence). Risk management and control functions can then concentrate on providing oversight and advice (second line of defence) and internal audit can provide independent assurance that the risk management programme is operating effectively (third line of defence).

Competent governance depends on the culture of the organisation, which in turn stems from the 'tone from the top'. Boards should therefore underline the need for business judgement to be taken within established risk parameters and lend their authority to ensuring risk is a paramount priority within the minds of frontline teams. Where risk management and control resources are limited, it is even more important that boards promote a culture of risk awareness and responsibility among frontline personnel. Recent experience also demonstrates the importance of both risk teams and senior management being prepared to challenge potentially detrimental risk positions.

4 CEIOPS: Advice to the European Commission on the Principle of Proportionality in the Solvency II Framework Directive Proposal, May 2008.

5 'Enterprise Risk Management and the Smaller Insurer', published by Standard and Poor's on 26.11.07.

6 'Enterprise risk management: ERM development in the insurance sector could gain strength in 2008', published by Standard and Poor's on 24.03.08.

7 'Does ERM matter: Enterprise-wide risk management in the insurance industry 2008', a study published by PricewaterhouseCoopers (June 2008). To download or order a free copy, please visit [www.pwc.com/insurance](http://www.pwc.com/insurance).

## Compliance management

The 'tone at the top' should encompass all aspects of governance, including compliance.

As policyholders become more informed and regulatory expectations become more exacting, insurers are facing increasing compliance demands in areas ranging from customer protection to outsourcing and anti-money laundering. However, compliance is now as much about safeguarding reputations as assuring compliance with formal regulation.

In turn, compliance functions are seen as an integral part of insurers' governance structures, augmenting and strengthening other aspects of control and risk management. However, many compliance teams are already straining under the escalating weight of managing both reputation and regulatory risk. There is a particular challenge in determining the scope of the compliance function's mandate within the overall governance framework and its differentiation from other risk and control functions.

Solvency II sees a permanent compliance function as an important control mechanism,<sup>8</sup> designed to advise the board and management on meeting current and future regulatory and legal requirements. At present, the latter is often allocated to the legal department. However, the directive's proposals may imply that insurers' compliance functions should also assume responsibility for ensuring conformance with prudential obligations. Such requirements are not as yet generally included in the remit of their bank and investment firm counterparts, though some supervisors do already expect the compliance function to be their main interlocutor. In effect, the detail of the

Solvency II proposals may blur some of the necessary delineation between compliance and risk management. It is therefore crucial that firms clearly define the compliance function's roles and responsibilities as part of the wider control framework.

The 'three lines of defence' approach outlined earlier can ensure that the various aspects of compliance are managed by the most competent and appropriately placed personnel. While retaining overall responsibility for key aspects of compliance, the compliance team can look to draw on the insights, experience and activities of other control and support functions. For example, risk management teams may detect lapses that might indicate a more pervasive pattern of non-compliant behaviour. HR can take the lead, with advice from the compliance function, in communicating expected behaviours, designing appropriate reward structures and, where necessary, determining disciplinary measures in line with the compliance culture established through the 'tone at the top'.

There are opportunities to align the risk management and compliance activities and sign-off procedures relating to sales practices, product design and strategic planning, along with the risk and compliance frameworks providing oversight of outsourced functions and activities. The benefits not only include more coherent controls through the elimination of separate risk and compliance silos, but also potential cost-savings in areas such as monitoring, documentation and disclosure.

As with risk management, meeting the compliance requirements of Solvency II may demand structural changes within the organisation. In particular, if compliance currently sits within the business legal department (transactions and deals),

companies may need to check whether any independence issues are created within such a structure. Moreover, while informal collaboration between different control functions may work in smaller organisations, larger firms need more formalised arrangements to eliminate potential overlaps, ensure that no risks are missed and maintain sufficient segregation.

## A platform for success

The need to maintain prescribed control functions and develop more systematic governance structures could place further demands on many insurers. There is no single approach or simple solution.

Companies need to carefully analyse the nature, scale and complexity of their individual risk profile and ensure that their associated governance framework is appropriate. They should also ensure that they have the formal structures and comprehensive documentation to satisfy supervisors of its appropriateness. At the same time, they need to look at how to leverage the control functions that already exist within the business to ensure that limited resources are targeted in the most efficient way and that the new governance requirements do not create a needless additional layer of corporate bureaucracy.

If effectively designed and applied, these organisational changes could provide a valuable opportunity to ingrain risk awareness into tactical decision making, strategic planning and the wider culture of the business. Clearly, some aspects of the business and its behaviour may need to be changed. However, at a time when any perceived lapses in compliance or control can wipe billions off share values, more systematic governance structures could help safeguard the value, reputation and franchise of the business. ■

8 Article 45(2) of the Framework Directive.