

Three lines of defence: How to take the burden out of compliance

AUTHORS: DENIS CAPRASSE, JULIEN LAURENT AND WENDY REED



At a time when stakeholders expect ever-more exacting standards of integrity and competence, compliance is now as much about safeguarding reputations and assuring strategic execution as ensuring formal regulation. Denis Caprasse, Julien Laurent and Wendy Reed outline how newly developed approaches to compliance risk management could help insurers to satisfy the demands of both regulatory supervision and public opinion, while enabling the compliance function to operate in a more focused, efficient and cost-effective way.

THREE LINES OF DEFENCE: HOW TO TAKE THE BURDEN OUT OF COMPLIANCE

With more and more regulations being imposed on the insurance industry, compliance functions are facing an increasing risk of overload and associated breakdowns in efficiency and delivery.

Yet, compliance now goes far beyond the narrow demands of regulation. The sub-prime lending crisis clearly shows how predatory sales practices, in this case offering credit to people with a limited capacity to repay, can have a punitive and potentially contagious impact on a financial services organisation's reputation, share price and ability to meet overall strategic objectives.

Although this lending was neither illegal nor non-compliant, it may have fallen short of the rigorous standards of integrity and internal control now demanded by investors, consumers and society as a whole. The compliance risk evident in such malpractice or comparable operational lapses was defined in a PricewaterhouseCoopers study as 'the risk of impairment to the organisation's business model, reputation and financial condition from failure to meet laws and regulations, internal standards and policies, and expectations of key stakeholders'.¹

As companies seek to meet these broad stakeholder demands, the compliance function is now recognised as an integral part of their corporate governance structure, augmenting and strengthening other aspects of control and risk management. However, this ever-widening remit can present organisational and operational challenges for already hard-pressed compliance teams.

Twin roles of compliance

A further challenge comes from the potentially conflicting roles of the compliance function within today's insurance companies – advising the business on the one hand and monitoring relevant activities on the other. Compliance teams need to find a careful balance between the fundamentally different mindsets and approaches required by the proactive 'trusted advisor' and the more reactive 'independent watchdog'.

The role of 'trusted advisor' tilts the focus towards preventive measures. This includes helping the business to anticipate regulatory intentions, correctly interpret and apply new regulations, thoroughly assess potential compliance risks, ascertain whether existing business processes are set up to operate in

a compliant way, and ensure that the business knows how to meet its obligations on a day-to-day basis. In a company where compliance risk management is well integrated into the business, this would also cover such proactive areas as early input into product design and approval.

However, the pendulum should not be allowed to swing too far in the 'advisor' direction. The compliance function also has a pivotal role in providing the necessary monitoring and oversight needed to assure senior management about the sound operation of the business. There therefore needs to be a clear delineation between active compliance and the necessary monitoring and oversight.

In the face of the increasing demands on compliance and the need for a clearer delineation of roles and responsibilities, a number of leading companies have adopted a more systematic and organisationally embedded framework for compliance risk monitoring and management. The framework aims to provide comfort for the business and the board, while reducing the potential strain on resources.



The framework aims to provide comfort for the business and the board, while reducing the potential strain on resources.

¹ 'Compliance: A gap at the heart of risk management', a report published by PricewaterhouseCoopers in November 2003 (www.pwc.com).

Effective monitoring

A compliance function needs efficient and effective monitoring capabilities, embedded in a resilient yet flexible compliance risk management framework, comprising three key elements:

1. Risk identification and assessment:

- Identification of threats to the company and the causes of potential loss and business disruptions;
- Assessment of the impact that a given threat may have on the company (based on quantitative methodology or on a qualitative approach);

2. Risk mitigation:

- The company takes various actions designed to mitigate the risk through the implementation of extra controls; or to reduce the impact of incidences;

3. Risk monitoring:

- Informing executive management about current and potential risks, enabling it to take suitable action and to monitor the risks and the effectiveness of mitigating measures.

The aim of the compliance risk management framework is to effectively monitor compliance risk across the business, continually validate the compliance risk assessment, evaluate the effectiveness of the mitigating measures in place and ensure that senior management has the information it needs to build compliance considerations into decision-making.

This framework can be adapted to any insurance company, while reflecting its specific size, scope and complexity. For larger insurers, we would recommend that the framework adopts a group-wide dimension, in order to:

- Ensure a consistent approach across business units;
- Maintain a simple and transparent process; and
- Allow flexibility to incorporate regulatory change.

Organisational integration

Compliance is not just the role of the compliance function; compliance needs to be embedded into day-to-day business operations in order to be effective. Equally, the practical constraints on resources mean that the compliance function may not be in a position to undertake all the tasks needed to ensure effective compliance monitoring. Leading practitioners have therefore developed a more robust and operationally comprehensive system of monitoring and control, based on three supporting lines of defence.

Business teams form the first line of defence through controls designed to ensure ongoing compliance is embedded into all relevant decisions and operations. Specified people within the business teams, ideally those not in the direct 'frontline', should be responsible for routine verification and providing the compliance function with up to date information on key risk and

control indicators (identified as part of the initial risk assessment process mentioned earlier).

The oversight provided by the compliance team, supported where necessary by other control functions, constitutes the second line of defence. This does not imply that the compliance function does no daily monitoring. In banks and investment firms, this daily monitoring activity focuses on particularly risky areas, such as suspicious transactions, market abuse, personal account dealing, etc. The compliance functions in insurance companies may need to monitor certain risks, for example those relating to conflicts of interest, on an ongoing basis. For other risks, the compliance function provides surveillance over the effectiveness of the compliance controls embedded in the business.

The third line of defence is internal audit, which undertakes independent and regular ex-post reviews of the overall compliance risk management framework (including the compliance function itself).

Collaborative process

Effective compliance risk management is a collaborative process that pulls together and leverages all the various control functions within the organisation, such as risk management, internal control, fraud detection, legal, human resources and complaints handling, ideally within an overall enterprise-wide risk management framework. This derives from the concept of 'centres of

competence'. For example, the risk management function could in the course of its duties help to detect potential compliance risks by identifying certain lapses that could indicate a more pervasive pattern of non-compliant behaviour. The human resources function is in turn the lead expert in managing people, including communicating expected behaviours, designing appropriate appraisal and reward structures and, where necessary, determining disciplinary measures.

While retaining overall responsibility for compliance in predefined areas,² the compliance team can therefore draw on the experience of other control functions. This collaborative approach can also help to eliminate wasteful duplication and promote information and knowledge sharing. However, there still needs to be clear delineation and ownership of specific responsibilities. Ideally, the compliance function should have a charter setting out its specific areas of responsibility. Arrangements for collaboration with other control functions can then be formalised into service level agreements (SLAs), which while in no way diluting the overall responsibility of the compliance function, can apportion certain tasks to the best placed 'lead' team.

Formal SLAs are especially advisable in larger, more complex or multinational organisations. These agreements should ideally seek to identify the potential synergies between the various functions and help strengthen the overall compliance risk management framework.

2 The EU rules for banks and investment firms clearly focus the compliance function's responsibilities on those regulations governing 'conduct of business' rather than prudential issues, which generally are the remit of risk management and finance functions.



Although more informal co-operation and collaboration between different control functions may work in smaller organisations, more formal SLAs could help to eliminate overlaps or prevent key tasks from ‘falling between the cracks’.

There is one major exception, however. The compliance function cannot delegate any of its monitoring tasks to internal audit as this would compromise internal audit’s position as an independent third line of defence (which includes monitoring the compliance function).

Visibility through dashboards

The compliance function’s monitoring tasks are split between those it undertakes itself and those carried out by others under its oversight. Thus it provides both the first and second line of defence in terms of different compliance risks. To enable it to do so effectively, it needs adequate monitoring tools. Compliance dashboards have become a popular tool for the ‘second-line of defence’.

The design of the dashboard derives from the underlying compliance risk assessment, a predetermined (by senior management) risk appetite or tolerance level, and an

assessment of the controls put into place to mitigate this risk (and the perceived effectiveness of that risk mitigation measure). Dashboards can be used to monitor the effectiveness of the compliance risk management framework within the business as a whole and also to monitor the effectiveness of the compliance function itself.

If well designed, their strength lies in providing ongoing, clear and early indicators of potential compliance deficiencies: a culmination of all the key risk and control indicators built into the overall compliance risk framework. Clearly, there may be a risk that the indicators are not

relevant or the information is skewed, ‘garbage in, garbage out’ as some cynics would term it. The indicators therefore need to be frequently and thoroughly reviewed to ensure ongoing validity, particularly in relation to the introduction of new regulations and requirements.

Optimal dashboards help visualise the effectiveness of the controls in real-time in order to proactively drive performance. This might include colour-coded ‘heat-maps’, which flash red on geographic or business-related compliance weaknesses. They can also generate ‘bubble-charts’, which indicate the magnitude of a potential risk, resulting from an

inherent control deficiency, or risk scores where the higher the score, the higher and more immediate the urgency for remedial action. The challenge is of course in the design. It needs to be sufficiently robust to be meaningful and helpful across multiple business classes and/or countries/regions, but also sufficiently simple and elegant that it will actually be implemented and used.

Dashboards developed to ascertain the performance of the compliance function itself need to:

- Ensure efficiency and effectiveness of compliance processes and procedures;
- Anticipate potential issues;
- Disseminate best practices; and
- Manage the total cost of compliance.

They can help the compliance function to measure the efficiency of their operations, processes

and staff against desired benchmarks aligned to the organisation's risk appetite.

Most dashboards use a variety of quantitative and qualitative measures of performance reflected in operational key performance indicators (KPIs). These can measure important objectives of the compliance operational performance and be classified by domains or areas, such as:

- Compliance department control and procedures;
- Compliance risk operating model;
- Independence assurance;
- Control on cost and budgets;
- Efficient HR and policies;
- Efficient IT support; and
- Reputation risk management.

Alternatively, the KPIs can be designed to focus on the compliance function's role within the overall governance of the organisation and ideally linked to other risk and control functions. Relevant KPIs, from this perspective, would include:

- Promotion of compliance to key function in the organisation;
- Building of a compliance culture;
- Interactions with business;
- Co-operation with HR department;
- Co-operation with internal audit department;
- Co-operation with legal department;
- Co-operation with risk management department;
- Co-operation with complaints handling department; and
- Co-operation with fraud department.

Raising the bar

The bar for compliance continues to rise as do the costs and, in some countries, the personal liabilities for breaches. To address this, compliance functions need clearly delineated responsibilities and disciplined approaches to compliance risk measurement and control.

A holistic and integrative approach to compliance risk management, incorporating a systematic three lines of defence and aided by accessible dashboard information, can help to instil a robust compliance risk management culture within the organisation as a whole. This includes embedding awareness and application of compliance into the business and leveraging competences between the various risk and controls functions. The result is a more assured, manageable and, not least, cost-effective approach to compliance. □

AUTHORS



Denis Caprasse

Director, Advisory Financial Services
PricewaterhouseCoopers (Belgium)
Tel: 32 2 710 7216
denis.caprasse@be.pwc.com



Julien Laurent

Advisor, Financial Services,
Governance Risk and Compliance,
PricewaterhouseCoopers (Belgium)
Tel: 32 2 710 7249
julien.laurent@pwc.be



Wendy Reed

Director, Pan-European Financial Services
Regulatory Advisory Services,
PricewaterhouseCoopers (Belgium)
Tel: 32 2 710 7245
wendy.reed@pwc.be



THREE LINES OF DEFENCE: HOW TO TAKE THE BURDEN OUT OF COMPLIANCE continued

