CLIFFORD
CHANCE

September 2011

Risk governance in the insurance sector – the role of the CRO and the board

The European Commission views corporate governance as a crucial tool for the prevention of future crises. The 2010 green paper for financial institutions, i.e., for banks and insurance companies, was clear on this. Green papers issued by the European Commission are intended to present initial thoughts and deliberations on a certain topic. Initial European measures stemming from the outcome of the consultation triggered by the 2010 green paper related only to banks, and not insurance companies as a part of the overarching group of financial institutions (draft CRD IV). This is not to say that it was decided to focus less attention on the issue of corporate governance in the insurance industry than in the banking sector. Banks are, however, clearly more closely intertwined with the financial market crisis and its triggers. Though the core business of the insurance companies did not contribute to trigger the financial market crisis, the crisis had a powerful impact on insurance companies, particularly with regard to asset management and regulatory consequences. It is interesting that in the draft CRD IV, the European Commission points out the necessity of increasing efforts at improving corporate governance not only within the banking sector but also – for consistency's sake – within the insurance sector as well.

Indeed, one of the core messages – demands, even – contained in the 2010 green paper will also be of particular relevance to insurance companies. In the European Commission's view, one of the lessons to be learnt in the financial market crisis is that it is necessary to enhance the status of the chief risk officer (CRO) of a financial institution (including insurance companies). A CRO must be more assertive than was the case during the financial market crisis. In that vein, the European Commission expressed the view that the chief risk officer should have "at least equal status to the chief financial officer". However, no demand is made that the CRO be a member of the executive board. Furthermore, the establishment of "close relations" between the chief risk officer and the (supervisory) board could also help to strengthen the role of the chief risk officer. The only way to interpret this is that, going forward, the CRO should no longer report to the CFO but rather directly to the CEO and he should have a duty to report directly to the (supervisory) board and its risk committee. The European Commission's deliberations could translate into the CRO being granted some sort of veto right in certain situations.

Before it was possible to formulate more detailed considerations on this topic to transpose this finding into the two-tiered German corporate governance system comprising the executive board and the supervisory board, the European Commission published another green paper in April 2011 dealing with corporate governance beyond the financial sector and (surprisingly) again addressed the issue of risk governance. In this new 2011 green paper, the scope of the (supervisory) board's responsibility with respect to a company's risk policy is put forward for discussion. The inclusion of the (supervisory) board in this matter is supposed to ensure the effectiveness, consistency and sustainability of risk governance.

The discussion in 2008 and 2009 of stronger regulation on remuneration, not only for executives but also for bank and insurance company employees in key functions, was already geared towards finding incentives to discourage short-term thinking and unwelcome risk-taking. This discussion addressed the core problem of risk; the aim was to prevent risk-takers, i.e., executives and individual employees in risk-taking positions, from exposing their financial institutions to inordinately high medium- and long-term risks in their pursuit of short-term profit.

In Germany, the Minimum Requirements for Risk Management in Insurance Undertakings (MaRisk VA), revised by the Federal Financial Supervisory Authority (BaFin) in 2009, stress that the executives of insurance companies are responsible for ensuring that "the undertaking-specific risk culture is systematically established and actually practised from the top level down". The objective must be to increase the risk-awareness of all risk-taking insurance company employees and to promote internal dialogue concerning risk management issues and risk transparency in general. BaFin takes a general approach to risk and risk management, whereby all elements of risk management must dovetail. On the one hand, there should be a top-down implementation of the risk strategy in daily operations in line with the risk profile. On the other hand, bottom-up reporting must be possible. BaFin calls this reciprocal reporting process "top-down/bottom-up planning". The overall risk profile of the company can be formed only through the interaction of these inverse information flows.

Legislation at the European and national levels has already dealt with the risk and remuneration complex at length. Risk has now been severed from the

discussion of variable remuneration at financial institutions and is being examined again and in detail, particularly also for listed companies outside the financial sector. The 2011 green paper makes it clear that the issue is no longer risk management – i.e., the structure of risk functions within the company – but rather the determination and implementation of a company-specific risk profile, an individual risk culture. Together, risk management at the operational level and a company's overall risk culture and risk profile can be best expressed with the new term 'risk governance'. The draft Solvency II Directive, too, pursues a risk-based approach intended to reflect the company's actual risk profile. The Directive uses the phrase "risk profile" more than 40 times.

But how can a company-specific risk profile be developed and anchored in the company's risk management structure in such a way as to establish and maintain the right form of risk governance as intended by the European Commission? It will be necessary to define the risk culture derived from the corporate strategy, to measure its acceptance among the employees and to ensure that all employees are mindful of the desired level of risk awareness in relation to business policy. The issue of risk culture should thus be placed on the executive agenda in order to bolster the meanwhile much-strained "tone from the top".

And now the European Commission is considering strengthening the role of the supervisory board in connection with fine-tuning the risk profile, i.e., company-specific risk appetite. However, the supervisory board's responsibility for the risk profile developed by the executive board must remain within the bounds of its authority under the two-tiered system. If one correctly interprets the demands made in the 2011 green paper, it is not up to the supervisory board to develop the risk profile itself and to derive from it an actual risk appetite, thereby determining the risk profile. Rather, the supervisory board should discuss the executive board's considerations on this matter internally as well as (at least with the chairman of the supervisory board as its representative) with the executive board. After doing so, it should weigh those considerations as the body responsible for the business strategy, and grant its consent (by way of resolution). Furthermore, the objective should be to reflect the practical risk of the company as it occurs in, for example, the remuneration structure, which falls under the (joint) responsibility of the supervisory board of a financial institution. In order to ensure that the company acts in a coherent manner so as to avoid risk mismatches and any discrepancies between its risk profile and the actual risks assumed, it is important to ensure that the company's risk appetite is in line with its ability to sustain risks. The company's business policy must be harmonised with its risk policy (risk alignment). Doing so would certainly be in the interest of good risk governance, and would not conflict with the customary division of responsibilities in the two-tiered German system.

Apart from the legislature and regulatory authorities, there are plenty of purely economic reasons to consider the suitability and quality of insurance companies' existing risk governance. Insurance companies are confronted with a vastly changing risk landscape: mushrooming complexity of business systems due to the diversity and heterogeneity of divisions and products, customer groups, distribution channels, countries, asset classes; rising volatility, primarily in capital assets; accelerating speed of product change, especially for life insurance products; the constantly more complex asset-liability management; the necessarily increasing pricing complexity; the "discovery" of new risks and interdependencies between risks (liquidity); cut-throat competition in saturated markets; the assumption of new risks in new markets, etc.

This situation, and not just in response to the current crisis, has driven insurance companies to begin analysing whether there is sufficient understanding and transparency with regard to risks, whether their risk appetite and strategy are sufficiently well founded and whether it is clear as to which risk culture should be strived towards and how they measure up. This in particular also applies to the governance issues derived:

- What is the mandate of the risk function and what is the CRO's role? How does the CRO go from being controller to advisor?
- How does one define the interfaces between CEO, CFO and CRO, and how will they function in practice?
- How should the interface with the supervisory board and its relevant committees be structured within the risk strategy and risk management issues?
- Which committees are responsible for risk issues, and what are their rights and duties?
- Do our employees and executives possess the requisite skills to manage our business risks?

Solvency II is a key ally in institutionalising the new role of the CRO. However, when it comes to implementing Solvency II, many insurance companies and CROs are currently focussing almost solely on the first pillar, i.e., the set-up and application of complex modelling capabilities and meeting compliance requirements. Yet CROs cannot fulfil their task within the meaning of the second pillar until they see themselves not only as guardians, but rather as active players structuring the company-wide risk culture and partners of management; i.e., helps it to adequately define their risk appetite and assists them in risk measurement, steering and management. Those insurance companies which, thanks to appropriate risk governance, are in a position to bear greater risk, will gain a key competitive advantage.

Authors

Daniela Weber-Rey
Partner at the Frankfurt office of Clifford Chance

Dr. Michael Ollmann
Director, McKinsey & Company, Inc., Hamburg

This article is a translation of an article which appeared in the German journal Börsen-Zeitung on 20 August 2011.

J201109090039437