

Reflections on Risk Management:  
Risk Management and Governance

Speech delivered by Mr. Arthur Philippe, Director of the Commission de Surveillance  
du Secteur Financier, at the PRIM 10th Anniversary Event (7 June 2007)<sup>1</sup>

It might be good news for you to hear that regulators have identified the need for a general framework for the regulations they have issued over time on the good functioning of a financial institution's machinery; this framework will be called "internal governance".

Good news is, that loose pieces like compliance and internal control, model validation and outsourcing, management duties and stress testing, can now be assembled in a global structure. Risk management is of course one important block in this building.

Good news also is, that there is an obvious, compelling link between "internal governance" and "corporate governance". That makes the building of internal governance, and with it Risk Management, a logical part of the corporate city, and it makes articulation, link-up and interaction between the different components more transparent and understandable.

I will not give you a full description of the regulators' work that is still under progress. I prefer to use 2 recent pieces of regulation, MiFID and Pillar II, to analyze in a bit more detail where the role of Risk Management lies and then derive from there some reflections on links between Risk Management, internal and corporate governance. Please do not misunderstand these latter comments as a comprehensive academic lecture on the topic.

On MiFID first.

MiFID requires from investment firms to comply with a set of operating conditions and organizational requirements, among them, the requirement for effective procedures of risk assessment. The risk management system should cover for instance the risks associated with the outsourcing of critical or important operational functions or the outsourcing of investment services and activities, just to give one example. These rules are designed to ensure a high level of integrity, competence and soundness in investment firms.

As general organizational requirements, MiFID asks among others to establish, decision-making procedures, internal control mechanisms and reporting lines.

---

<sup>1</sup> This speech has been prepared with the collaboration of Messrs Edouard Reimen and Claude Wampach, CSSF

With regard to Risk Management, investment firms are requested to have in place adequate risk management policies and procedures which identify the risks relating to the firm's activities, processes and systems, and to set the level of risk tolerated by the firm. They are expected to manage the risks relating to the firm's functioning in light of that level of risk tolerance.

Where proportionate with the nature, scale and complexity of their business, firms have to establish a risk management function that operates independently and carries out the implementation of adequate policies and procedures, and which reports and gives advice to senior management. An investment firm which is not required to have such an independent risk management function, must nevertheless be able to demonstrate that the policies and procedures which it has adopted satisfy the regulatory requirements and are consistently effective.

What I described to you and what you will read in a Level 3 circular that we are preparing, is not really new. It is in a sense plain vanilla language on organizational matters that you find in many types of prudential regulations.

There are however 2 noticeable differences between MiFID Risk Management and Risk Management requirements as they exist in a different context, like capital adequacy or market and credit activities.

First, Risk Management, when dealing with MiFID policies, procedures and processes, will have to deal with a specific kind of risk, which is the risk of providing inadequate products and services to customers. I mention as examples best execution policy, inducements, suitability and appropriateness test, conflict of interest policy.

Secondly, the requirements of MiFID Level 1 and Level 2 are generic, in fact of a very principles-based nature. But the CSSF will not issue at Level 3 detailed technical Guidance on all the aspects I mentioned before. So, the concrete procedures and risk tolerance levels in an investment firm will have to be derived from a voluntaristic strategy developed by the firm rather than from a true and fair transposition of rules into the firm's system. Be assured that supervisors will evaluate the firm's approach in this respect.

In the absence of precise rules, developing this strategy in line with MiFID is to a large extent a responsibility of each individual investment firm and a task for Risk Management, not for compliance as one might think at first reflection. I will explain it in more detail later on.

\* \* \* \* \*

Lets move to Pillar II as another example of upcoming requirements of interest to the RM function.

Pillar 2 of the Capital Requirement Directive requires institutions to operate an Internal Capital Adequacy Assessment Process (or ICAAP). The ICAAP is the means by which institutions identify and measure the risks to which they are exposed and determine internal capital needed to support these risks. The resulting internal capital adequacy has to cover all the risks the institution is exposed to and, consequently, complements the prudential capital adequacy under Pillar 1 which requires prudential capital to be held against certain types of risk only.

ICAAP represents a true challenge for risk managers. Risk identification requires indeed a deep understanding of all the activities undertaken by an institution, how they perform under different, presumably extreme, market conditions and how they interact. Furthermore, there are risks that are difficult to measure or to assess like for instance compliance and reputational risks arising out of private banking or investment fund related activities. Let aside the methodological issues, the practical implementation of ICAAP raises issues regarding data availability, data quality and reporting lines. Model risk is omnipresent as approximations, shortcuts and second best solutions are unavoidable. But how robust are they?

Unfortunately, you will, just like for MiFID, not find comfort in the great book of prudential regulation. Indeed, the CSSF circulars 06/273 and 07/290 emphasize that ICAAP is an internal process, defined, implemented and operated in a way to primarily serve the institutions' own and specific needs. Therefore neither the CSSF nor other European supervisors intend to issue detailed prescriptions on how the ICAAP has to be designed, implemented or operated, which does not mean that we would not be open to an exchange of views and systematic dialogue on the subject. The circular on ICAAP, that we presently have under preparation, will not be an easy book of well tested recipes in this respect.

However challenging the ICAAP might be for risk managers, it provides them with unique opportunities to strengthen their expertise and their voice, both within their institutions and outside, for instance to the benefit of stakeholders taking a look at the institution's risk/return profile.

The key risk indicators that allow stakeholders to adequately perform their assessments are best provided by competent risk managers acting with the required independence. In accordance with the internal nature of the ICAAP, the institutions' internal processes of risk identification, measurement and reporting are the same processes that feed into the ICAAP demanded by the regulator. The risk managers' output thus becomes increasingly visible both internally and externally.

His contribution is a central element in the sound and integer implementation of ICAAP by senior management, the embedding of ICAAP into the institution's control environment including the internal audit and the compliance function, as well as in the involvement of the board in monitoring ICAAP.

\* \* \* \* \*

Keeping these two topics, MiFID and ICAAP, in mind, one comes across a number of more fundamental questions on the structure which relates Risk Management to governance. I have picked out 2 of them to comment on.

The first aspect is on Risk Management and the Board of Directors' implication, or, to put it differently, on Risk Management and corporate governance.

For Directors it is a story of love and hatred, considering the support and assurance they receive from Risk Management but considering at the same time that their implication means in fact their responsibility. The relation between the Board and the Risk Management function is indeed ambivalent and ambiguous in practice. A widespread conception is that the managers are the main if not the sole depositories of the Enterprisewide Risk Management function; such a conception could indeed easily be derived from an agency theory approach. Directors would thus not carry any direct responsibility for internal governance.

But let us look more closely at the question of why Directors should be involved in Risk Management issues and to what extent. I will do it by building on 2 essential responsibilities entrusted on Directors in a Corporate Governance perspective.

First, Directors represent the interests of shareholders. Now, where do shareholders stand with respect to Risk Management? They expect to be remunerated by a premium for the supplementary risk of investing in a single asset rather than in a diversified portfolio; indeed, they are not able to mitigate their investment risk by way of diversification and therefore rely on the firm to do it on their behalf. Directors have in this respect a duty to reduce the volatility of profits for the sake of stabilizing the intrinsic value of the investment made by the shareholders, and to reduce the volatility of dividends for the sake of the foreseeability of future returns, meaning the market value of this investment.

Second, Directors represent the interests of the firm itself and of stakeholders other than shareholders. The interests of the firm are that "survival" is delivered to it so that it can develop its specific skills, make that its competitive position in the market is guaranteed and possibly improved and that its financial position is strengthened.

The interests of other stakeholders in a model where ownership and management are separated are, that firms operate at economically acceptable agency costs, that enterprises act in a socially responsibly way and that economic efficiency does not jeopardize political objectives. As such, their interests are in line with those of the shareholders.

How can these finalities be obtained better than by a high standard of Risk Management. Risk Management reduces the risk of failure and distress and creates efficiency in the production process. Risk Management also protects the financial position against self seeking behavior of the market, the clients and the firm's management. Risk Management helps serve the interests of the community at large by creating secure employment and by creating value, part of which comes to the society and its democratic role.

Moving towards these high-level goals should however not be conditional upon shifting all Risk Management responsibilities to the Board of Directors, loading in fact managerial duties on the shoulders of those who are its controllers. The question therefore is, while recognizing a clear Board responsibility for Risk Management, how it should be articulated with the Management's responsibility for the same function.

In order to assume its role as the depository of the governance process, the Board must practice guidance and oversight in an efficient way.

To start with, risk management must be embedded in governance practices and strategic planning. A Board's role is to agree on objectives and strategies and to communicate on them. The Board can contribute here its expert judgment.

It is also incumbent to the Board not only to fix the risk tolerance thresholds but also to set the tone for ethical behavior.

An enterprise wide framework of Risk Management, whose structure has been conceived by the Board, has to be implemented under its oversight. Once the framework has been put in place and authority has been assigned to the management to manage the risks on a day-to-day basis, the Directors' role will be to keep themselves informed on a regular basis, -should this apply through its audit committee-, on the risk profile, its management and the performance of risk limitation mechanisms. It is obvious that corrective action has to be taken at this juncture.

What I told you in the last few sentences is corporate governance and good prudential behavior at the same time. You will therefore not be surprised to read this kind of views in our upcoming regulation on ICAAP and MiFID.

What it means for Risk Management is that this function is not only at the service of the management but also at the Directors' service. Risk Management is therefore part of Corporate Governance, Corporate Governance being a collective exercise of Directors, Managers, external audit and all those who act in the control line of an enterprise: internal audit, compliance and risk management.

But, is Risk Management really a control function by nature? I will give you some views on this second more fundamental topic by turning back to basic governance thinking.

Remember that the Board has a genuine management role in addition to its control function. Risk Management, at the service of Directors, must then follow. Indeed, it has as a central role to link growth and return to risk.

Under such a broad conception, Risk Management cannot remain confined to a compliance function of a sophisticated type, stepping in when it comes to formulas, square roots and intricate structured products.

In a joint project with the Economist Intelligence Unit, PWC has made a study on this subject and has issued a warning at the end of their report: there is a widespread

thinking that investment into Corporate Governance and Risk Management means stepping up compliance.

This observation is extremely worrisome indeed. It means in fact that regulators become risk managers and risk managers are regulators' watchdogs on the spot.

To cast it into an equation:

Risk Management = high compliance with rules = deference to the regulator

Such a solution would fall extremely short of the aim and the benefit of good governance, and this for several reasons:

- First, a regulatory approach and intervention remains elusive by nature.
- Secondly, rules should be principles based; if they are rules based, they invite to exploit loopholes and shortcomings and they will be weak and failing at the end of the day.
- Thirdly, experience demonstrates that public oversight has often been inefficient and malfunctioning.

Risk Management as a cornerstone of good governance, must therefore not be shaped merely to avoid or limit trouble, but it should contribute to improve the quality of management. In other words, it must be instrumental in exploring an optimal and responsible utilization of the firm's resources. Risk Management must manage upside risks, not only downside risks.

I hope you understand now, that all these reflections make us as a regulator prudent in venturing to deep into Risk Management requirements. On the other hand, regulation calls for strong Risk Management, even more so when you look at the two pieces of ICAAP and MiFID I have presented to you.

But both regulations leave room for interpretation and well-advised application. If we do not wish to fall in the trap that PWC has identified in their study, we better refrain from regulatory fill-up of this empty room, but leave that to governance and risk management.

This leads us to a different equation:

Risk Management = better management = good governance = satisfied and relaxed regulators.