Financial Law Institute

Working Paper Series

WP 2012-04

Eddy WYMEERSCH

Risk in financial institutions – is it Managed?

UNIVERSITEIT GENT

January 2012

WP 2012-04

Eddy WYMEERSCH

Risk in financial institutions – is it Managed?

Abstract

Adequate Risk management has become the central pre-occupation of financial regulators, central banks, and banks as well. Awareness about the risk issue has increased considerably, partly spontaneously, partly under the pressure of new regulations, esp. the Basel III standards. Risk measurement – "risk appetite" is a management tool, a process and a learning curve, more than a fixed formula. Risk inspired restrictive measures abound, but may overly reduce the credit flow to the economies, making it difficult to strike the right balance between risk stability and liquidity provision.
The Basel II- CRD IV call special attention to risk management by introducing some very clear cut rules, leaving the traditional comply and explain approach to a stricter supervisory intervention. Should a bank adopt its behavior if this may potentially trigger macro-risk? What is the role of the auditors and of the shareholders dealing-opposing strict risk management. More work has to be undertaken, but banks obviously are investing considerably in better risk controls.

Instituut FINANCIEEL RECHT FINANCIAL LAW Institute

© Financial Law Institute, Ghent University, 2012

UNIVERSITEIT GENT

Although the banking crisis of the latter half of 2011 can be attributed to the legacy of the years 2007-2009, new flaws have appeared, leading to serious concerns about the overall concept of today's banking business[1] Specific incidents like the occurrence of rogue trading, causing undeniable damage to the system and its credibility, along with continuous concerns about misselling, both at the asset side and with respect to investment products cause considerable damage to the reputation of the financial sector as a whole. Therefore a reflection on the way banks handle their risks, and how risk management relates to the overall governance structure of the banks aims at giving an overview of the state of the art these days, with some recommendations for future strengthening.

The subject of risk management has been extensively analysed and discussed in numerous statements by national European and international banking authorities[2], all calling for a stricter risk oversight structure, more elaborate and detailed procedures and finer analytical work. Private organisations have analysed in great detail the techniques of appropriate risk management as practised in large banks these days. All this has lead to a new perception where "risk" is the master of the game.

1. Risk awareness

Looking back to pre-crisis times one of the striking evolutions of the last years is undoubtedly the very strong interest for risk management. Issues that were on the forefront of discussions before 2008, such as financial conglomerates, Basel 2 implementation or shareholder value have not faded but are overwhelmed by the key focus on risk issues. This is clearly reflected in the increasing number of statements, recommendations, legislative proposals and other initiatives dealing with risk in its multifarious aspects. The number of bodies that have 'risk' on the top of their agenda is impressive: IMF, World bank, BIS and BCBS, European Commission, CEBS and now EBA have laid the groundwork for a comprehensive if not always very well coordinated drive for radically improving risk techniques, procedures or internal structures. In addition and at the more detailed practical level, one should mention the statements of the Senior Supervisors Group, the numerous detailed "guidances" on risk management organisation published by the national supervisory authorities , and from the industry side, the reports and publications by the Institute of International Finance, the organisation regrouping the world's major banks. The implementation of much of these new recommendations is still under way, and although significant progress has been made in the banks' internal rules, the actual roll out will still require further time, efforts and budgets.

Looking at these numerous reports, statements, recommendations, codes of conduct[3], and guidance, one can only conclude that the risk issue has now become central to all developments in the banking sector. This concern has partially taken up by the markets as well: some of the riskiest pre-crisis products have more or less disappeared: see securitisation, CDOs and other synthetic products, but they may now be replaced by exchange traded funds that being offered to the retail investors may bode even greater danger. At the same time risk measurement tools have been improved e.g. under the form of risk indices, or even as CDS. All this results in more risk awareness, and should contribute to lower the risk profile of the financial institutions.

---

[1] See the famous statement of A Turner calling some of the City's activities ' socially useless'

[2] see: the numerous documents from the Basel Committee; Senior Supervisors Group, Risk Management Lessons from the Global Banking Crisis of 2008, Oct 21, 2009.On the broader subject of internal governance, see EBA guidelines on Internal Governance 27 September 2011.

[3] See IIF, Principles of Conduct and Recommendations in Final report of the Committee on Market Best Practices, July 2008, updated December 2009 in Reform on the Financials Services Industry: Strengthening Practices for a more Stable System, December 2009.

At the same time, risk in financial institutions changed in nature from a risk profile based on the analysis of the individual institution to overall or macro risk analysis, translated in notions as financial stability, or even as systemic risk. Risk is not longer perceived as the risk of the individual institutions, but includes an overarching risk factor that may affect several individual institution or even the financial system as a whole. This change in perspective is translated in a change in terminology from "prudential supervision" to "macro-prudential supervision". It took place in the early 2000s and lead to a significant overhaul in the structure of financial supervision putting the central banks in the centre of the supervisory network. Systemic concerns dominate today in banking regulation but also in the field of alternative investment funds, of market organisation, of exchange traded funds, etc. In order to cope with this new challenge, new institutions dealing with systemic risk and overall financial stability have been created addressing the aggregate situation of the individual financial institutions, and especially the linkages between them and the other factors that may trigger risk contagion between otherwise independent legal entities[4].

The very significant drive to reposition the banking system as a major, in several respects systemic risk bearer raises the question whether this evolution does leave sufficient room for the traditional business functions of the banks, i.e. the distribution of the credit and organization of payment systems. If the excesses of the past cannot be excused, one should be aware that too much prudence may lead to burden economic recovery and even put in danger the banks' ability to recover from the past and still undigested losses. Here the best may be the enemy of the good.

Along with this evolution one can fear that most of the activity that banks are now refrained from undertaken will move to other, less regulated sectors. This is the issue often referred to as the "shadow banking " question, a wholesale terminology covering a very wide diversity of financial and quasi- financial firm.

Although not all financial activity should be covered by the same rules, there is clearly a need for an all encompassing regime of oversight allowing to understand developments in sectors that are usually not covered by traditional prudential regulation. The principle should be that no financial activity escapes the sharp eyes of the financial supervisors. Often the alternative investment funds are pointed at in this context: as far as Europe is concerned, the recently adopted directive on Alternative Investment Fund Managers would contain sufficiently detailed instruments to deal with risk developments up to the level of systemic concerns.

But one should broaden the view to developments outside the financial sector: risk management in non-financial firms is equally important and may be as devastating. Examples from the oil industry, or from the nuclear sector illustrate this concern: is a ban on nuclear energy the only valid response?

2. The role of the board in risk management

It is now widely accepted that the board has an active role to play in overseeing and monitoring the risk management structure within the bank, on the one hand by requiring the management to propose an appropriate and efficient risk management policy, including the development of a Risk Appetite Framework allowing for the identification of risks both on a firm wide basis and per business line, and on the other the introduction of the supporting IT schemes that will allow top management and the board to gain a timely and comprehensive insight in the risk apprehension, at any moment and on an evolutive basis, for each of the business lines and allowing for corrections where due. On the basis of this overall insight, strategic decisions can be made.

[4] See about the methods of identifying these links: Financial Stability Board, Understanding Financial Linkages: A Common Data Template for Global Systemically Important Banks 6 Oct 2011

At the level of the overall organization of the bank, the proposed directive CRD IV recalls these organizational duties[5], and requires the banks' board to constitute within its ranks a risk committee, thereby formally embedding the risk approach in the overall bank's governance[6]. Although several of the larger banks already had instituted a "risk committee", or a "risk and capital committee", the rule would now be applicable to all banks, although smaller institutions could organize the function within the board itself without organizing a separate formal committee. The risk committee is composed of non-executive directors, and not so much of independent directors as high levels of technical expertise are required. The committee should be composed of persons with good knowledge in the field of risk strategy and capable of judging the risk appetite of the firm. The risk committee acts as an expert advisory body to the board, meaning that the committee will essentially ensure the follow-up of developments in the Risk Appetite framework, but the formal and ultimate decisions belong to the board. This would especially apply if the board had to take position on certain derogations from risk limits, or their transfers from one business line to another. The risk committee should establish a close dialogue with - and encourage dialogue among -the top managers responsible for risk matters i.e. the CEO, the CFO and the CRO.

The committee is expected to oversee the introduction of a robust risk culture within the bank. This consists of the introduction of a "risk function" being a vertical risk line established throughout the entire organization. The directive also mandates the designation of a Chief Risk officer (CRO[7]) defining his status and position within the firm, further the introduction of procedures and guidelines for rendering the business lines and their leaders aware about the risk framework, require the management to develop the necessary IT tools and data collections that will allow to capture risk developments, both within the firm, and in the markets, and culminating in the determination of the "risk appetite", one of the core notions in today's approach to risk . In these new development the notion of "risk appetite" plays a crucial rule: it has been defined as " the amount and type of risk that a company is able and willing to accept in pursuit of its business objectives", taking into account the appropriate or pursued returns. It is to be distinguished from "risk capacity" as this is the amount of risk a firm is willing to support given its capital, liquidity position etc. but also taking into account losses and negative events that can reasonably be calculated. Per definition, risk appetite should not exceed risk capacity and if that would occur, the necessary adjustments have to be made whether by lowering the risk position or by increasing the risk capacity. It also points to the way the firm wants to be looked at by its different stakeholders, including its employees, regulators, the rating agencies.

Defining the risk appetite is a complex process, more of a learning curve in which the different players will get better and better acquainted with the sometimes very intricate risk positions and the equally complex ways to mitigate these risks[8]. Its validity is verified in ex post stress tests.

The latter is a complex exercise that has been described more of a learning process than a firm or rigid determination of risks

[5] Proposal for a directive, "CRD IV," 20.7.2011 Com (2011) 453 final, 2011/0203 (COD), esp. art.75. "Ensure effective and prudent management of an institution" and further "the management body shall have the overall responsibility for the institution, including approving and overseeing the implementation of the institution's strategic objectives, risk strategy and internal governance". These rules are addressed to the "management body", what would include the board in the unitary systems and the management committee in the two tier systems.(see 5.3 of the Explanatory memorandum to the CRD IV; compare EBA Guidelines, nt.2, at 10)

[6] About this committee, see Hartmann, Wolfgang Aufgaben und Rolle des Risikoausschusses von Banken in Hopt and Wohlmannstetter (eds) , Handbuch Corporate Governance von Banken, Vahlen Beck, 2011,528-582;

[7] See: Schmittmann, Stefan, Die Rolle des Chief Risk officer under Corporate Governance Gesichtspunkten, Hopt and Wohlmannstetter (eds) , Handbuch Corporate Governance von Banken, Vahlen Beck, 2011,528-582 481-492.

[8] This aspect is highlighted in: IIF, Implementing robust risk appetite frameworks to strengthen financial institutions June 2011

The risk policy requires on the one hand the risks to be identified, assessed and evaluated throughout the organization, but on the other calls for a follow-up in terms of monitoring the business lines. Although essentially pursued from a risk perspective, it can be powerful driver for unlocking value by pursuing a netter alignment between decision-making and risk. Both activities are within the remit of the risk management line, that cuts across the entire organisation, and although remaining in close dialogue with the operational staff, ultimately reports to the chief risk officer or CRO. These risk officers, that are part of the management, determine the risk centers, identify the probability and volume of the risk, prepare the risk appetite statement and in some matters may even be entitled to intervene in the actual business operations on the basis of risk considerations, although the latter point is quite controversial[9]. The risk oversight staff should also be able to act independently, and not be subject to the instructions of the department heads. Its action should cover the entire organization and include all subsidiaries, at least those that are consolidated in the accounts. The risk oversight staff should have access to all information within the bank, and able to collect the necessary information from the operational staff and draw up risk charts that will feed into the risk appetite statement. For all these reasons its legal and functional position has to be defined by the board.

The breadth of their tasks and their sometimes difficult relationship with the operational line raises the issue of the legal and factual position of the risk officers, and especially of the Chief Risk Officer (CRO) in the organisation of the bank. His position is a balancing act between action and control. He will normally be of a sufficiently high ranking,[10] member of the executive[11], usually taking part in the meeting of the executive body and contributing to its significant esp. strategic decisions, but sufficiently independent so that he can criticize decisions of that body without being fully subject to the views of the CEO or of the executive. This would mean that his appointment, or at least his dismissal should take place with the board's agreement, or in case of his resignation with the board being adequately informed[12]. On the other hand he should have a direct reporting line to the risk committee, who can request him to present reports on specific items. But he remains part of the executive, and insures the permanent dialogue of his risk staff with the leaders of the business lines.

The risk policy is not indifferent in terms of labor relations and remuneration policy: the policy should be consistent with effective risk management and not encourage risk-taking that exceeds the level of tolerated risk[13]. Apart from the remuneration debate at the level of top management,

[9] This point has not been stated in this way in the CRD IV proposal, but may be good practice. CRD IV defines the function as "identifying, measuring, and reporting on risk exposures". But it states that the CRO should involved "in all material risk management decisions", what might mean that he would not be involved in the business decisions themselves. Compare in the similar sense: EBA Guidelines on Internal Governance, nt.2, 27.4

[10] "which shall have sufficient authority, stature, resources and access to the management" and "independent senior executive with distinct responsibility for the risk management function body" according to art.75(5) of the proposed CRD IV

[11] This is the case in 92% of the top 25 European banks according to an investigation in Nestor Advisers Ltd.: Bank Boards After the Flood, Oct 2010, p. 12. In a world wide survey covering 60 large banks, IIF and Ernst and Young found 86% having constituted a separate risk committee: Making strides in financial services risk management. And strikingly, the board approves the CRO's remuneration in 72% of these cases.

[12] No removal "without prior approval of the management body", states art. 75(5) of the directive. This risk committee would normally play a first hand role. But his appointment is not necessary a board matter, at least according to the directive.

[13] Art 88(2)(a) CRD IV.

some firms use promotion and compensation on the basis of adherence to the Risk Appetite Framework[14]

3 Banks' governance and macro risks

In principle banks as corporate entities are subjects to the general corporate governance rules, varying depending on whether their shares are traded on the public markets or not. This regime can be considered a default regime, as banks and financial institutions are held to much more demanding standards in terms of good governance due to the fact that they carry an important part of public confidence and create considerable negative externalities for depositors, creditors and society at large. Some decisions may trigger wider risks, usually referred to as contagion risks that may take on the dimension of systemic risks. This is often considered as affecting only the largest financial institutions, the SIFIs or the G-SIBs as they are called today. Contagion can develop from relatively small events – suspension of reimbursement of investment fund shares– that shake market confidence, or disrupt the regular function of trading in a market – the flash crash e.g. Most larger individual banks or financial firms should ask themselves whether and how their action can lead to significant contagion, and hence to systemic developments.

Reformulating the question in terms of corporate governance, this would mean that boards of directors have to ask themselves whether their decisions – and worse, their non-decisions- may affect these wider, often unfathomable risks, and as a consequence adapt their own decision, if needed subordinating their direct financial interest to the public interest at large.

In theory and according to the traditional analysis, private companies are not accountable to the public interest: they only serve the interests of their investors – shareholders and creditors - and of their other stakeholders as the latter would usually also benefit the shareholders' interests. Identifying what belongs to the public interest and how this has to be achieved belongs to the tasks of the public authorities, legislators or regulators. If firms have to respect certain rules of general interest, these should be imposed by law or regulation. We all know that in reality matters are not that simple….

To what extent should firms include these wider - especially contagion - risks in their internal decision-making? Could a firm and its directors be held accountable for having taken decisions that were manifestly detrimental to the financial system as a whole, or to a country's Treasury? The answer will usually be negative, as the nature of this obligation will be too undetermined, and the bank's board or management would first have to honor its duties – including fiduciary duties – towards its investors and shareholders. Only in view of clear and legally based instructions from the state bodies would the answer be different.

Beyond a strict legal analysis however a bank may take into account its wider responsibility to the community within which it operates. The balance will be difficult: can the bank prefer in crisis situation to withdraw foreign exchange from its subsidiaries abroad, putting the host state in difficulty? And what about shorting the host state's bonds in order to protect own's assets? In a longer term perspective the bank may need to take account of these wider interests in order to safeguard and protect its reputation and standing in its host community.

The proposal for a new Capital Requirement Directive seems to include the follow-up of some macro risks in the overall description of the board's tasks, where it states that

"Competent authorities shall ensure that the management body approves and periodically reviews the strategies and policies for taking up, managing, monitoring and mitigating the risks

[14] See SSG, Observations on Developments in Risk appetite frameworks and IT Infrastructure, December 23, 2010, report, p. 9 citing as incentives, career advancement, but also dismissal for those who disregard the framework.

the institution is or might be exposed to, including those posed by the macroeconomic environment in which it operates in relation to the status of the business cycle. "

This reference to the "business cycle" could be read as relating to the pro-cyclicality measures that are alluded to in other provisions of the directive, but does not clearly impose banks to take responsibility for the externalities that may be caused by macro events.

In the absence of a clear legal relation, the link between macro-prudential policy and bank management needs further analysis. Public authorities are in the process of developing tools allowing the identification of negative evolutions in the field of systemic risk: in Europe, the recently instituted ESRB is in charge of identifying these risks and will if needed issue recommendations and warnings. These are addressed to the European Supervisory Authorities or ESAs who should then transmit the information to their members, the national supervisory authorities. It is unclear to what extent the latter authorities can require banks of financial institutions to adhere to these policies other than by the explicit regulatory or prudential measures, for which often there will be no legal basis. A certain number of tools exist already and have been practiced by governments in many jurisdictions: these range from adapting loan-to- value ratios, reducing exposure limits, imposing transactions taxes, restrictions on certain risky products, prohibit certain foreign currency borrowing, strengthening lending criteria, and ultimately provisions and capital[15]. Although most of these instruments have been introduced for other objectives than macro-prudential ones, e.g. consumer protection, market stability or creating tax revenues they have undeniable effects on financial stability and risk reduction. These measures should all be based on explicit legal bases, and cannot be subsumed to be included in the generally formulated business purpose of a bank. Beyond these explicit measures, recommendations for other measures that are not provided for in the regulation may be needed. Given the prominent position of the Financial Stability Board, financial institutions would be well advised to heed its recommendations, even if these are not legally binding.

4. Risk management tools: "risk appetite"

Developing a *risk appetite framework* is not a simple assignment: by introducing an all pervasive awareness for risk, in sharp contrast to the previously pursued objective of return on assets, it constitutes something like administering a culture shock. The exercise involves the entire firm but allows for some diversity for specific businesses or risks for each if its business lines. Being largely based on quantitative models resulting in limits that are familiar or at least easily understood by staff, it also incorporates qualitative elements or unquantifiable risks that are more difficult to explain or to justify. The operational staff has to be closely involved in the exercise, for fear that it would consider to be solely bound by the restrictions, based on whimsical justifications, or seen as not justified at all, especially as it may directly affect their financial position. Moreover the exercise is expensive, time consuming and requires a lot of sometimes innovating brain work. For these reasons, it is frequently underlined that the exercise cannot be successful if it is not strongly supported by the entire organization, by the board, top management and the heads of the businesses lines who explain and convince their staff about the need of the framework and becomes part of the overall firm culture in order to obtain adherence from all staff levels.

There is not one single methodology for measuring a bank's risk appetite, and even within a group there may be differences although differences in approaches should at least remain consistent. Nestor Advisors identified two different methodologies, a first one being essentially quantitative in terms of strategic guidance bases on a classical risk-return trade-off, the second

[15] CGFS, Macroprudential instruments and frameworks: a stocktaking of issues and experiences, Paper 38, May 2010; see IIF, Macroprudential Oversight, July 2011,esp. p. 9 e.s. An Industry perspective, Submission to the International Authorities, p.22.

more based on quantitative elements fixing boundaries for acceptable risk. The qualitative method used i.a. by the major French banks – gave little guidance to risk takers and may expose the bank to bottom-up pressures from their part. The simplest methods essentially put targets to the different risk categories as have been defined, and may be completed by qualitative measures such as reputation, compliance with regulation, management motivation. The more elaborate qualitative instruments usually are based on financial targets, such as capital, rating, earnings volatility, liquidity ratio, regulatory standing[16]. Economic capital is used as a measure for determining the capital needs for different levels of unexpected events: stress test and scenario analyses are put at work in this approach. For some segments of the activity of a bank, e.g. exposures to credit risk figures are already published. Other methods as Value at Risk or VAR are frequently used and stressed and should be handled with the usual caveats.

The entire exercise results than in a formal risk appetite statement that is put forward by the executive board, and the highlights of which are submitted to the board for final approval. It establishes the boundaries as fixed ultimately by the board within the different departments can act, given the proposed strategy. The document is not published according to present practice although some annual reports give very detailed information on the risk management in general.

A few essential guidelines should be followed when using the risk appetite as a management tool. There should be a good understanding of the objectives of the exercise, that is never to be considered final and always open to review, refinements and new methods. The risk appetite is part of and should be closely linked to the main decision strategy, and to finance planning. Beware for a mathematical approach: formal limits give a misleading impression of safety and exclude further discussion. Contingency measures remain necessary and escalation has to be provided for.

Beyond these technical aspects, the board should have a good general understanding of the risks involved in the overall business of the financial institution. Some aspects have been spelled out in generally accepted statements of the prudential authorities such as the Basel Committee. Although these statements essentially address the management, the board bearing the ultimate responsibility should remain vigilant. One such example is the “know your structure “ rule. The board should have a clear understanding of the structure of the group of companies that form the financial institution. Although some complexity cannot be avoided, it should be a concern that the group structure has become so complex that it is opaque, leaving pockets of risk in invisible or impenetrable corners of the group. Special attention deserve important unconsolidated subsidiaries, as was illustrated in the CDO crisis. This point will deserve special attention once the practice of introducing “living wills” will become more widespread.

“Know your customer” is another maxim of prudent banking, essentially addressed to the management. But a vigilant board cannot be insensitive to the regulatory reputation risk that may be caused from banking with undesirable clients.

5. Types of risks

Dealing with risks is first and foremost the task of the bank itself that should develop appropriate policies and strategies for identifying the risks, manage, mitigate and monitor them, however under the attentive eye of the supervisor.

Most types of risk are well identified and the mitigation and evaluation methods are widely known[17]. The proposed directive contains a list of different risk types, stating for several of them some additional requirements. The proposal obviously does not consider this list as conclusive, as new types of risk are likely to appear over time. Moreover some risk type have

[16] See for the relative importance of these different factors according to the observations by KPMG Australia, Understanding and Articulating Risk Appetite, 2008

[17] Some of these and their methodologies have been dealt with in the CRD, implementing the Basel 2 Accord.

not been expressly mentioned, but are considered to be included in the widely defined categories: there is no mention of reputation risk or systemic risk as such, as these are probably seen as the incremental phases in the existing types, IT risk and legal risk would normally qualify under the general heading of operational risk, but will have to be considered separately as key ingredient of the overall risk determination process.

A short overview of the approach of the proposed directive is worthwhile as it illustrates the concerns at the moment of drafting

- Credit and counterparty risk[18]. Credit institutions are urged to assess these risks themselves – including for default and migration risk – and develop internal ratings based approaches and not rely exclusively on credit ratings[19].
- Residual risk[20] referring to the existing methodologies and techniques that are less than perfect. This might include tail risk.
- Concentration risk[21] for which written policies and procedures are required, but no overall figure is mentioned.
- Securitisation risk[22] including reputation risk and provision of liquidity plans for amortisations
- Market risk where attention is drawn to risks of a shortage of liquidity for short transactions
- Interest risk arising from non-trading book activities[23]
- Operational risks[24] with special attention to low-frequency high-severity events, and reference to contingency and business continuity plans. Key risk indicators allow management to be alerted about impending problems and take mitigating action. Often these risks are unpredictable and not quantifiable: legal risk reputational risk. They are usually quantified according to the AMA approach under CRD. Mitigation through insurance has been mentioned.
- Liquidity risk has received detailed attention. Institutions shall communicate risk tolerance to all relevant business lines and per state where business is carried on.
- Risk of excessive leverage[25] referring to the leverage ratio determined in accordance with Article 416 of the CRD Regulation

Legal risk deserves more attention and has not been very well explored. It is difficult to recognize ex ante, shows up many years later, ultimately after the courts have handed down their final decision, and often a long time after the board and management have left. The causes can be very subtle (nullity of contracts, unsatisfactory disclosure, biased advice) but the consequences sometimes are destructive for the bank and may even reach a systemic dimension[26],.

[18] Art. 77 CRD IV
[19] "In particular, internal methodologies shall not rely solely or mechanistically on external ratings. Where own funds requirements are based on a rating by an External Credit Assessment Institution (ECAI) or based on the fact that an exposure is unrated, institutions shall use their own methodologies in order to assess the appropriateness of the rank-ordering of credit risk implicit in those own funds requirements and take the result into account in their allocation of internal capital" art. 77 (b)
[20] Art.78
[21] Art.79
[22] Art.80
[23] Art 82
[24] Art,83
[25] Art 85
[26]. Striking example of legal risks with systemic dimension are found in the Netherlands, the so-called Legio Lease Affair (equity leasing contracts, see: nl.wikipedia.org/wiki/Aandelenlease-affaire), or in the case of the "woekerpolissen" (usurious policies) see nl.wikipedia.org/wiki/Woekerpolisaffaire, the latter potentially gravely damaging a large part of the insurance sector. More recently about the use of interest rate swaps with local communities (Province of Pisa, Consiglio di Stato, Sect V, nr 5032 of 7 July 2011, or with unsophisticated investors (Ille Papier, Bundesgerichtshof Decision of 22. 3. 2011 - XI ZR 33/ 1) that in both cases were held

Some risks are rarely discussed and deserve some attention. The risk from shareholders is an good example: that the rating of a financial institution can affect its owners speaks for itself, but also the opposite may happen, e.g. if the shareholder's rating is downgraded (eg a sovereign state) of has become insolvent putting the institution into play. Reputation damage or conflict of interest situation may also affect the reliability of a bank, especially in states where relations with shareholders are opaque, or where dominant shareholders use their position for exacting considerable private benefits of control[27].

6. Involving the auditors?

It is striking that in much of this debate the intervention of the auditor is rarely mentioned. This can mainly be explained on the basis that developing a risk policy is essential an internal management matter, that aims at steering and alerting management, but is less the basis for the external communication that is the outcome of the auditor's activity. However there can be little doubt that many of the assessments in the Risk Framework are highly relevant to the auditor's analysis of valuations and risks: therefore the auditor should at least have access the reports and findings developed as part of the Risk framework. The SSG, in its original report, drew attention to the need to involve the auditors without further clarifying to what extent and in which way the auditors should be involved.

When auditors use the data relating to an audited institution, according to the ISAs they should first "perform risk assessment procedures to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion level[28]". This assessment is an essential step for guaranteeing the integrity and reliability of the published data.

7. Involving the shareholders?

It is equally striking that the debate about risk management takes place with little or no reference to the shareholder, although in today's corporate governance discussion he is in the centre of attention. Obviously this seems due to the fact that risk management is essential a management issue, the management acting under the overall oversight of the board. But one can certainly not state that the importance of risk management is disregard by the shareholders, but annual reports of financial institutions – at least of the best ones – do pay considerable attention to the bank's risk management.

A first useful analysis would consist of differentiating depending on the ownership structure of the company. In smaller banks, mostly with concentrated ownership, one can assume that the controlling shareholder keeps a close eye on the risk evolution of his bank. But most large banks, especially due to their strong needs for capital, will be based on a dispersed ownership structure, in which the direct role of the shareholder is very limited, his oversight being essentially exercised through the members of the board. Therefore the selection of candidates for board positions is crucial and should strive to identify candidates that as non-executives, are "sufficiently knowledgeable and have the necessary skills and expertise to understand the risk strategy and the risk appetite"[29]. These conditions apply to all members of the risk committee

---

invalid but leading to fear of massive damages.

[27] See for the effects of private benefits on the pricing of the shares: Gilson R, Controlling Shareholders and Corporate Governance: Complicating the Comparative Taxonomy, Aug 2005, ECGI - Law Working Paper No. 49/2005,,

[28] See International Auditing Standard (ISA),315.5

[29] Art. 77(3)

and one can fear that it will be hard to find the appropriate persons, having sufficient technical insight and expertise in the firm's overall environment, for meeting said conditions. Practically only former bankers will qualify. Questions may arise with respect to former officers of the bank, as one may fear that they would adopt a somewhat biased judgment on issues in which they were themselves involved. The proposed directive only requires that the members of the risk committee should be non-executive, not that they should be independent.

The shareholders are informed about the bank's principal risks in its annual report. When the company is using financial instruments, the financial risk management objectives and policies, and its exposure to price risk, credit and liquidity risk and cash flow risk have to be included in the annual report[30]. For listed companies this is done pursuant to article 46 of the 4th directive, and implementing national regulations. Moreover for listed companies the report should contain a description of the main features of the company's internal control and risk management systems, in relation to the financial reporting process[31]. The Guidelines by CEBS – now EBA – on Consolidated Financial Reporting do not contain a specific reference to this point[32].

Conclusion

The development of an elaborate risk management function, especially with its panel on risk appetite is still a relative recent phenomenon. The implementation in the different banks is still under way and is likely to require further development taking into account the considerable IT investments that have to be made. Where we stand mid 2011 in the process of introducing a reliable Risk Appetite framework depends on the source of information: in December 2010, the Senior Supervisors group wrote that significant progress has been made in " conceptualizing articulating and implementing a risk appetite framework" But these improvements leave some doubt whether " firms will have advanced these practices sufficiently to be resilient in an increasingly competitive and changing regulatory environment". It was mainly on the point of aggregating risk data that the SSG identify as the main challenge laying ahead[33]. A more positive voice is heard from the industry, recognizing that more work remains to be done but citing figures illustrating that about 4/5th of the large banks have taken the necessary measures, but that remaining hurdles were due to "organizational silos, decentralization of resources and decision making lack of integrated data management and delivery and inherent complexities of operating globally"[34]

[30] Art.46 of the 4th Directive on company law
[31] art 46 a 1. C of the 4th Directive on company law
[32] Guidelines for Implementation of the Framework for Consolidated Financial reporting, (FinRep), March 2009
[33] SSG, nt.10, p.14; see also IIF and McKinsey, Risk IT and Operations, Strengthening capabilities, 21 June 2011.
[34] Ernst and Young and IIF: Making strides in financial services management, 2011

Financial Law Institute

The **Financial Law Institute** is a research and teaching unit within the Law School of the University of Ghent, Belgium. The research activities undertaken within the Institute focus on various issues of company and financial law, including private and public law of banking, capital markets regulation, company law and corporate governance.

The **Working Paper Series**, launched in 1999, aims at promoting the dissemination of the research output of the Financial Law Institute's researchers to the broader academic community. The use and further distribution of the Working Papers is allowed for scientific purposes only. Working papers are published in their original language (Dutch, French, English or German) and are provisional.

© Financial Law Institute
Universiteit Gent, 2012

More information about the Financial Law Institute and a full list of working papers are available at:
http://www.law.UGent.be/fli