THE ROLE OF THE RISK CONTROL FUNCTION UNDER THE BASEL II FRAMEWORK

Thomas Dietz

Abstract

While the financial turmoil has left the business approach of ethical banks unchanged, as evidenced in the striking stability of their balance sheet from 2007 to 2009, the pattern shown by big banks has substantially changed over this same period. These developments would tend to suggest the need to reform the business model of big banks. There is no clear empirical evidence that a banking system with a large number of small institutions would be any more stable than the system as it currently stands. Besides, financing certain big projects would always require the existence of large international banks. Both types of financial institutions are in fact complementary. How to regulate the banking and financial sector is thus a complex and multifaceted issue. One cannot impose the same requirements on big international-oriented banks and small domestic banks. As this paper has tried to demonstrate, both have a distinct business model.

The following statements and assessments represent the author's opinion only. They should not be interpreted as official statements or assessments from Deutsche Bundesbank.

> *"[…] risk monitoring and management reduces to the basics of getting the right information, at the right time, to the right people, such that those people can make the most informed judgments possible."*[24]

If a bank wants to earn money it has to take risks. From an economic point of view this is a good thing to do. In a world without banks and without institutionalised financial markets each consumer would need to look for a potential counterpart he could lend money to (savings he currently doesn't need) and would need to bear the risk of his contract partner's insolvency personally. Conversely, enterprises willing to invest in the real economy might be restricted by not finding enough consumers to collect the amount of money needed for these investments. Even if they do so, these consumers might not be willing to lend their money long enough.

Financial intermediaries are lowering transaction costs in the economy as a whole, take over counterparty credit risk from their depositors and fulfil important maturity transformation functions. This is especially important for emerging markets like the countries from central, eastern and south eastern Europe (CESEE countries) where financial markets have only started to develop. Taking risks is not enough, however. For permanent financial stability it is equally important that banks are able to survive stress situations in which risks have become virulent. Otherwise depositors will lose their confidence in the sound functioning of financial markets causing a shortage of savings needed to refinance investments.

Financial regulation aims at minimising the risks for financial stability. For this purpose supervisory authorities all over the world have implemented rules that are supposed to mitigate banks' insolvency risk. Under these rules banks have to hold enough capital and liquidity to survive stress situations. To guarantee a level-playing field for banks (and for banking supervisory authorities!) worldwide the Basel Committee on Banking Supervision (BCBS) has published a framework for Capital standards and Capital measurement (called Basel II[25]) on credit, market and operational risk and several complementary guidelines, for instance on the management of liquidity or on stress testing. On the European Union level two directives have been adopted that implement the Basel II framework. The Banking Directive (2006/48/EC[26]) sets minimum capital requirements for credit and operational risk, the Capital Adequacy Directive (2006/49/EC[27]) minimum capital requirements for market risk. Both directives are subsumed under the term "Capital requirements directive" (CRD).

However, holding enough capital and liquidity under a regulatory perspective might still not be enough. Even well capitalized institutions have gone bankrupt (or have come close to bankruptcy) in the past because they have become victims of rogue traders like Nick Leeson from Baring's Bank or

[24] Counterparty risk management group (2008), p. 70.

[25] BCBS (2006a).
[26] EU (2006a).
[27] EU (2006b).

Jerome Kervel from Société Général[28]. In such cases risk management has had some serious shortcomings. On the other hand, if risk management in a credit institution is sound, capital and liquidity cushions might not need to be that strong since taking certain (excessive) risks is either avoided completely or risks are managed in a way that they do not become excessive at all. In that respect, a sound risk management is the first line of defence against a bank's possible bankruptcy. Consequently, the Basel II framework also contains some rules concerning risk management in general and an independent risk control function in particular.

The following article takes a closer look at these provisions and – primarily driven by the financial crisis - at current suggestions for strengthening these rules further.

Risks in financial institutions

Risk management plays a decisive role within financial institutions. Risk identification, risk measurement, risk control and risk management in a narrower sense (in terms of hedging, reducing or completely selling off risky positions) are crucial for institutions which business it is to earn money by taking risks without being killed by those risks.

The most important risks a bank is facing are

- credit risk
- operational risk
- market risk
- liquidity risk

Risk as a general concept is symmetrical and simply means that actual outcomes differ from expectations. For instance buying a share for 100 € with the expectation of selling it for 120 € three months later bears a downside risk (the value of the share then is lower than 120) but also an upside risk (what would typically be labelled as the "chance" of showing a value higher than 120).

The banking supervision community has a biased view on risk. In their terms risk always means potential losses (and never potential gains). Under this perspective credit risk is the risk that a counterparty to a financial obligation, such as a loan, will default on repayments linked to the obligation causing losses at the creditor. Operational risk according to Article 4 section 22 of the Banking directive means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Market risk is the risk that investments will lose money due to fluctuations in market prices like interest rates, stock values or exchange rates. Finally, liquidity risk is defined as the risk that a bank is not able anymore to fund increases in assets and meet obligations as they come due, without incurring unacceptable losses[29].

The Basel II framework

The Basel II framework is divided into three different so-called pillars. For the first three types of risk mentioned above Pillar I sets some minimum capital requirements the banks have to comply with at all times. However, for other risks like liquidity risk, concentration risk or business risk there are no such requirements. The same holds true for interest rate risk in the banking book. Thus, when it comes to capital requirements, there are some risks that are not or at least not completely covered (like concentration risk as part of credit risk) under Pillar I.

For those kinds of risk Pillar II (the "Supervisory Review Process" – SRP) sets some requirements concerning a bank's internal processes aligning the total of risks it has taken to the capital it holds internally as a cushion against these risks. This "Internal Capital Adequacy Assessment Process" (ICAAP) is monitored and reviewed by the supervisory authorities taking into account the principle of proportionality (the more important the bank and the more complex its business the more often and the more detailed it will be monitored by the supervisor). As a result of this "Supervisory Review and Evaluation Process" (SREP) the supervisors might impose some additional capital requirements exceeding those under Pillar I.

However, as the Basel framework points out, the SREP should not only make sure that banks hold adequate capital to cover all the risks in their business, but also to "encourage banks to develop and use better risk management techniques in monitoring and managing their risks."[30] This is because capital cannot be regarded as a substitute for addressing shortcomings in the bank's risk control or risk management processes. Moreover, liquidity risk – especially in crisis situations - is not mitigated by holding capital against it at all.

Furthermore, under the SREP the supervisory authorities have to assess whether or not the banks do comply with some minimum standards for the more advanced risk measurement and management methods in Pillar 1, particularly the so-called IRB framework for credit risk, the Advanced Measurement Approaches (AMA) for operational risk and (typically) Value-at-risk models for market risk. In all these cases the minimum capital requirements depend on bank's internal estimations of potential losses assuming a certain stochastical confidence level. The adequacy of the minimum capital requirements therefore depends on the accuracy of parameter estimations used to calculate these losses.

[28] For some interesting background information on the most important financial losses of banks and other companies in the 1990s see Jorion (2001), p. 15-21.

[29] BCBS (2008), p. 1

[30] BCBS (2006a), p. 204.

A good way to guarantee this is a strong internal governance structure.

As a general approach, Basel II allows for lower capital requirements when using advanced methods compared to the standardised approaches for credit, operational and market risk respectively. However, since the supervisory authorities need to grant approval for the use of these models first, and since approval will depend on the compliance with some qualitative minimum requirements also referring to risk control and risk management processes, the price the banks have to pay for lower capital requirements are higher costs for risk management. Basel II therefore has increased the sophistication of risk management within banks.

To complete the picture, the third pillar of Basel II sets some disclosure requirements for the risks banks have taken. It is supposed to "encourage market discipline by developing a set of disclosure requirements which will allow market participants to assess key pieces of information on the scope of application, capital, risk exposures risk assessment processes, and hence the capital adequacy of the institution."[31]

The institution's internal governance structure

A bank's risk control function is part of a broader internal governance structure comprised of

- the management body
- senior management
- the risk control function
- the internal audit function

Several international institutions have published guidance on internal and corporate governance aspects, inter alia the BCBS[32], the OECD[33] or the industry-based Institute of International Finance (IIF)[34]. Also some national authorities like the british Treasury have only recently joined the crowd here (Walker Report)[35].

On the EU level the London based Committee of European Banking Supervisors (CEBS), a coordinating and advisory body for the national banking supervisory authorities and for the European Commission, has issued guidance on this topic, too[36]. As a "Level 3 Committee" CEBS is part of the Lamfalussy procedure, a specific comitology procedure established to speed up legislation on financial integration in the EU. CEBS recommendations are not legally binding yet. However, this will change as soon as it has been transformed into the European Banking Authority (EBA), one of the three European Supervisory Agencies that are supposed to be established at the beginning of 2011 following the recommendations of the so called De Larosière Report[37].

Under the Banking Directive Internal Governance is referred to in Article 22 and in Annex V. It aims at ensuring that an institution's management body is explicitly and transparently responsible for the bank's business strategy, organisation and internal control procedures and is concerned mainly with

- setting the institution's business objectives and its appetite for risk
- how the business of the institution is organised
- how responsibilities and authority are allocated
- how reporting lines are set up and what information they convey
- how internal control (including risk control, compliance, and internal audit) is organised.

An example for a possible internal governance structure is given in Figure 1. In this example the Risk Control function reports to the Chief Risk Officer (CRO) being a member of the management body. Since the CRO does not take positions that bear credit, market or liquidity risks for the bank the Risk Control function is located independently within the governance structure of the bank. Since Internal audit is also controlling the control functions within the bank (like the Risk control function) Internal audit should not report to the CRO. Instead it reports directly to the CEO.

In this graph the management body represents the top (executive) management level of the bank as circumscribed in Article 11 of the Banking Directive. Senior management should be understood to represent the level of management directly below the management body, like the head of Compliance or the head of Risk control in our example. This classification is complient with the CEBS Guidelines on the Supervisory Review Process[38] (GL 03) and the Guidelines on the implementation, validation and assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) approaches (GL 10)[39].

However, this classification is not the only one on the market. For instance, the Basel II framework defines "senior management" as the highest executive body in a bank and the "board of directors" as the highest supervisory body (supervising the executive body). These deviating definitions are due to the different institutional solutions around the globe when fulfilling the two key functions in an institution: management and supervision. Most EU member states for instance use one of two corporate

[31] BCBS (2006a), p. 226.
[32] BCBS (1998; 2006b).
[33] OECD (2004).
[34] IIF (2008).
[35] HM Treasury (2009).
[36] CEBS (2006a; 2006b; 2009)
[37] The High level Group (2009).
[38] CEBS (2006a), p. 6.
[39] CEBS (2006b), p. 103.

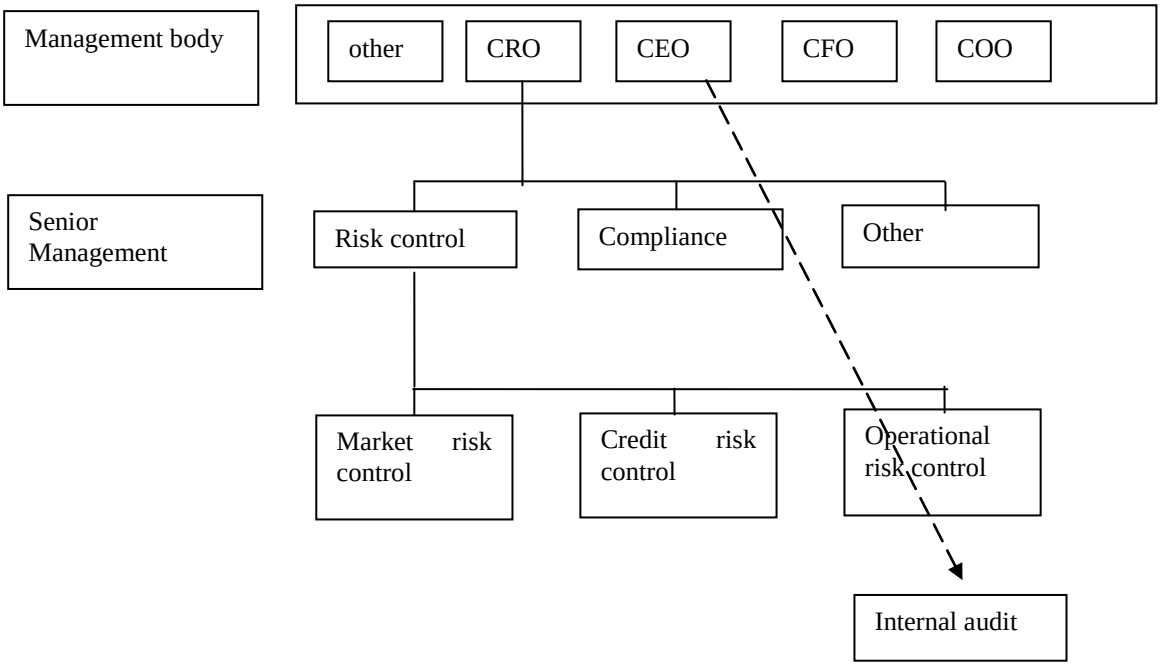
governance structures: a unitary or a dual board structure. In a unitary board structure, one body (e.g. the "board of directors") performs supervisory and management functions at the same time (by allocating management and supervisory functions to different persons respectively), whereas in a dual board structure the two functions are performed by different bodies[40].

Getting it to the right people - The management body and senior management

The management body bears the overall responsibility for almost all aspects of the banking business. It cannot be expected therefore that each member of the management body is an expert for each field the bank is conducting business in. Nor should it be made a requirement that the members of the management need to understand each technical detail of risk measurement systems like a sophisticated rating system. However, they must have a basic understanding of the risks the institution is taking in order to take informed decisions concerning the risk profile of the institution. According to the two CEBS guidelines mentioned above the management body is responsible for (inter alia)

[40] BCBS (2006a), p. 205 and CEBS (2006a), p. 6. For the sake of simplicity in the following we do not distinguish between the supervisory and the management function of the management body when describing its responsibilities. Details on this can be found in the respective Guidelines themselves.

Figure 1. Example for an internal governance structure in a bank



CRO: Chief Risk Officer
CEO: Chief Executive Officer
CFO: Chief Financial Officer
COO: Chief Operating Officer

- understanding the nature and level of risk taken and its relation to adequate capital levels
- setting the bank's tolerance for risk (taking into account all relevant risks including off-balance sheet transactions)[41]
- the strategic planning of (i.a.) the bank's capital needs and the bank's access to external funding sources
- setting and enforcing clear lines of responsibility and authority within the institution
- documenting risk strategies and policies with the help of written guidelines, manuals and other means
- monitoring and periodically assessing the effectiveness of the institution's internal governance structure
- developing strong internal control systems providing for adequate segregation of duties in order to prevent conflicts of interest (for instance banking supervisors would not accept a member of the management body responsible for the trading activities of the institution being at the same Chief Risk Officer)
- overseeing senior management[42]
- setting regular and transparent communication mechanisms for the sharing of information about risk measurement, analysis and monitoring[43], e.g. by setting up risk committees
- setting compensation schemes that discourage "unhealthy risk taking or maximisation of short term profits"[44], both for the management body and lower down the management chain (including the sales and trading function level)

Especially the last point has become crucial for supervisors in the aftermath of the financial crisis, since excessive risk taking was encouraged by short-termed profit- but not risk oriented compensation schemes. Several initiatives have been launched both on the European and the international level to foster more sustainable compensation schemes in the future.

There are several other lessons to be learned from the financial crisis when it comes to internal governance. As the Senior Supervisor's group points out, banks having suffered least from the crisis are the ones where the above-mentioned principles were respected, inter alia since

- risks were managed under an integrated, firm-wide approach with good communication across several risk management teams
- an authoritative CRO was in place

[41] CEBS (2010), p. 4.
[42] CEBS (2010), p. 3.
[43] CEBS (2010), p. 6.
[44] CEBS (2008a), p. 477-481.

- information was passed swiftly upwards to the management body[45]

There are enough examples, however, where these principles had not been taken into account:

- information about (excessive) risk taking did not reach the management body or senior management
- members of the management body had approved a risk strategy but did not establish suitable metrics to monitor its implementation[46]
- banks' management bodies took strategic decisions to retain large exposures to super senior tranches of Collateralized Debt Obligations (CDOs) without understanding the risks inherent in such investments
- a number of management bodies were not aware of senior management or even lower management levels taking risks beyond the risk appetite set by the management body
- it was difficult to persuade the management body to pay sufficient attention to the results of forward-looking stress testing
- there was a lack of systemic procedures for escalating red flags to the management body[47]

Not only CEBS, also the Banking Directive itself makes direct reference to the management body, for instance when it comes to Internal Ratings Based Approaches. According to Annex VII Part IV paragraph 124 of the Banking Directive the management body has to approve all material aspects of the rating and estimation processes. Furthermore the management body needs to have general understanding of the credit institution's ratings systems and detailed comprehension of its associated management reports. In order to improve the understanding of the rating system and to improve the efficiency the management body may delegate certain aspects to specific risk committees.

However, as the CEBS Guidelines point out, this does neither relieve the members of the Management body from their obligation to have a general understanding of the IRB framework nor from its ultimate responsibility for developing and implementing it[48]. The same holds true for the use of an Advanced Measurement Approach for calculating the capital requirements for operational risk[49]. Furthermore, according to CEBS the management body holds ultimate responsibility also for

- policies and key procedures in relation to exposure to concentration risk
- the overall stress testing framework
- the proper management of the risks associated with outsourcing[50]

Finally, when it comes to liquidity risk, Annex V of the recast Banking Directive calls for robust strategies, policies, processes and systems for the identification, measurement, management and monitoring of liquidity risk, proportionate to the complexity of the institution's business the and liquidity risk tolerance set by the management body[51]. In addition to this, according to the 2008 CEBS Advice to the Commission on liquidity risk management the management body needs to have a sound understanding of the tools used to measure liquidity risk and the results of stress tests, being able to take appropriate action if necessary[52].

Senior management

Senior management is responsible for risk management on a day-to-day basis but still on a rather highly aggregated level of risk. On the other hand, for senior management a deeper knowledge of technical details of the risk measurement and management system compared to the management body should be expected. In particular, senior management should ensure that the institution sets trading, liquidity, credit and other risk limits based upon the institution's risk appetite[53]. For instance, when it comes to IRB systems Pragraphs 124 to 127 of the Banking Directive set the following requirements: Senior management shall

- possess a general understanding of the credit institution's rating systems and detailed comprehension of its associated management reports
- provide notice to the management body or a designated committee thereof of material changes or exceptions from established policies that will materially impact the operations of the credit institution's rating systems
- have a good understanding of the rating systems designs and operations
- ensure, on an ongoing basis that the rating systems are operating properly
- be regularly informed by the credit risk control units about the performance of the rating process, areas needing improvement, and the status of efforts to improve previously identified deficiencies.

Furthermore, in the case of an IRB approach, the CEBS guidelines 10 call for a good understanding of credit policies, underwriting standards, lending practices, and collection and recovery practices, and

[45] Kirkpatrick (2009), p. 69.
[46] Kirkpatrick (2009), p. 62.
[47] Kirkpatrick (2009), p. 67-71.
[48] CEBS (2006b), p. 104.
[49] CEBS (2006b), p. 135.
[50] CEBS (2008a), p. 488-489.
[51] EU (2009), p. 116.
[52] CEBS (2008b), p. 44.
[53] CEBS (2010), p. 4.

should understand how these factors affect the estimation of relevant risk parameters. When it comes to operational risk, senior management should adequately assess operational risk inherent in new areas (products, activities, processes, and systems) before they are introduced, and identifying risks tied to new product development and other significant changes in order to ensure that the risk profiles of product lines are updated regularly[54].

In general, senior management should ensure that the following tasks are being addressed:

- Ensuring the soundness of risk taking processes
- Determining how internal ratings are used in the risk taking processes
- Identifying and assessing the main risk drivers, based on the information provided by the Credit Risk Control Unit or the Operational Risk Management Function
- Defining the tasks of the risk control or risk management function and evaluating the adequacy of its professional skills
- Monitoring and managing all sources of potential conflicts of interest;
- Establishing effective communication channels in order to ensure that all staff are aware of relevant policies and procedures;
- Defining the minimum content of reporting to the management body or to bodies to which it has delegated responsibilities (e.g., the Risk Committee), and
- Examining reports from Internal Audit or another comparable independent audit unit[55].

Senior management should also check, on a regular basis, that the control procedures and measurement systems adopted by the credit risk control unit and Internal Audit (or another comparable independent audit unit) are adequate and that the overall IRB system remains effective over time[56].

Getting the right information at the right time - The risk control function

If senior management or the management body is supposed to "*make the most informed judgments possible"* these judgements must be based upon correct and timely information. The more independent the unit to which risk control functions are allocated the higher the probability that the right (i.e. not manipulated) information can indeed be delivered at the right time. Conversely, the more this unit depends on the risk taking units in a bank the higher the likelihood that unfavourable information will be hidden or completely oppressed and that the management body will never see it (or will only get aware of it when it is too late to rescue the bank like in the case of Nick Leeson). One of the painful experiences some banks had during the financial crisis was indeed that the proximity of risk managers to traders was (too) high[57].

It doesn't come as a surprise therefore that all guidelines covering aspects of a risk control function call for the independence of this function from the business lines it monitors and controls. According to the CEBS Guidelines 03 a control function can generally be regarded as independent if the following conditions are met:

- The control function staff do not perform any tasks that fall within the scope of the activities that the control function is intended to monitor and control
- The control function is organisationally separate from the activities it is assigned to monitor and control.
- The head of the control function is subordinated to a person who has no responsibilities for managing the activities that are being monitored and controlled.
- The head of the control function reports directly to the management body and/or the audit committee, and is present at least once a year at meetings of the body it reports to.
- The remuneration of the control function staff is not linked to the performance of the activities that the control function is intended to monitor and control.

As already mentioned before, it is the responsibility of the management body to ensure that the risk control function has sufficient resources, well-qualified and experienced staff, as well as a sufficient number of staff. Since an organisational separation or, in general, meeting all of the above conditions may not be practical for smaller institutions, the CEBS Guidelines explicitly allow for taking other measures to safeguard independence as long as the institutions can show how any real or potential conflicts of interest are avoided or mitigated.[58]

This is exactly the reason why the CEBS Guidelines generally speak of an independent risk control function and not of an independent risk control unit (like the Banking Directive – see below) – this unit might not exist! Or a bank might not choose "risk control" but "risk management" (which would usually be aligned with risk-taking activities!) as the name for a unit being responsible for risk control functions. Finally, the risk control functions might be spread over two or more different organisational units[59].

[54] CEBS (2006b), p. 136.
[55] CEBS (2006b), p. 105 and 136.
[56] CEBS (2006b), p. 105.
[57] Kirkpatrick (2009), p. 71.
[58] CEBS (2006a), p. 16-17.
[59] CEBS (2006b), p. 107.

But what exactly would be the tasks of an independent risk control function? The Banking Directive defines these tasks for institutions applying an AMA or an IRB approach quite clearly. According to Annex VII Part IV Paragraph 128 the "Credit risk control unit" shall

- be independent from the personnel and management functions responsible for originating or renewing exposures
- report directly to senior management
- be responsible for the design or selection, implementation, oversight and performance of the rating systems
- regularly produce and analyse reports on the output of the rating systems.

Paragraph 129 provides further details on this. Also CEBS offers some more responsibilities like backtesting and benchmarking the predicted parameters (Probability of default, Loss given default, Credit conversion factors) against third party data sources[60].

Similarly, according to Annex X, Part III Paragraph 3 of the Banking Directive the credit institution must have an independent risk management function for operational risk. Again, the CEBS Guidelines 10 elaborate further on this: The Operational risk management function (ORMF) should have sufficient resources and skills in operational risk management and measurement methods and knowledge of the processes of the institution and is responsible (inter alia) for the following aspects:

- The operational risk measurement methodology
- Monitoring systems
- Reporting
- Operational risk quantification and allocation processes
- Backtesting and benchmarking, and the methodology for allocating operational risk capital to subsidiaries[61].

Furthermore, if an institution uses an internal model for calculating the minimum capital requirements for market risk, the Capital Adequacy Directive (CAD) requires in Annex V Paragraph 2 inter alia that

- the institution has a risk control unit that is independent from business trading units and reports directly to senior management.
- this unit must be responsible for designing and implementing the institution's risk management system and shall produce and analyse daily reports on the output of the risk measurement model and on the appropriate measures to be taken in terms of trading limits.
- this unit shall also conduct the initial and on-going validation of the internal model;
- the institution's board of directors and senior management are actively involved in the risk control process and the daily reports produced by the risk control unit are reviewed by a level of management with sufficient authority to enforce both reductions of positions taken by individual traders as well as in the institution's overall risk exposure;
- the institution has sufficient numbers of staff skilled in the use of sophisticated models in the trading, risk control, audit and back office areas;

One important point in all these requirements seems to be reporting directly at least to senior management. The establishment and maintenance of management information systems that cover the full range of its activities is indeed a critical component. This information is typically provided through both electronic and non electronic means. Management decision making could be adversely affected by unreliable or misleading information provided especially by systems that are poorly designed and controlled[62]. Again, the independence of the function being responsible for the reporting process is therefore crucial.

Recipients of internal reporting should at least be senior management and (typically less frequently and less detailed) the management body. The frequency and content of reporting will in general depend on an institution's size and the complexity of its business and should be formally approved by both the management body and senior management.

The minimum requirements of the CRD relating to IRB reporting are specified in Annex VII, Part 4, Paragraphs 126 and 128. CEBS provides some examples for what this could include:

- A description of the rated portfolios (amounts, number of obligors, PDs per grade, percentage of coverage with ratings with respect to the total portfolio, breakdown by entities, sectors, subportfolios, and business units)
- The distribution of the overall portfolio according to rating grades, PD bands, and LGD grades, and a comparison with the previous year
- A comparison of realised default rates (and loss given default and credit Conversion Factors for institutions on advanced approaches) against expectations
- The results of stress tests[63]

[60] CEBS (2006b), p. 107.
[61] CEBS (2006b), p. 138.
[62] CEBS (2006a), p. 18.
[63] CEBS (2006b), p. 106.

For operational risk calculated with the help of an Advanced Measurement Approach reporting could include:

- New or improved management policies, procedures, and practices (e.g., changes in the business environment, business practices, and internal control factors);
- Risk reduction and risk transfer strategies (e.g., the effect of any expected loss deductions, cost benefit analysis of insurance policies, mitigation and corrective actions on the business line/event type exposure and/or losses, cost benefit analysis of the mitigation actions);
- Operational risk exposure (e.g., description of key operational risk events and drivers, and the distribution, trend, and migration of the operational risk exposure across business lines);
- Internal and (where relevant) external loss experience (e.g., event type loss analysis and comparison in term of trends, seasonality, geographical distribution, etc.);

Furthermore, the CEBS Advice on liquidity risk management stresses the importance of an efficient reporting system, too, as "[…] the quality of the reporting process is essential to ensuring that the management body and senior management have a sound understanding of the tools used to measure liquidity risk and the results of stress tests, and that they are able to take appropriate action if necessary."[64]

As the examples listed above show, the CRD offers similar requirements concerning an independent risk control function whenever it comes to the use of internal models for the calculation of minimum capital requirements. However, there is no need to go further into details of other risk models made reference to in the CRD, since the examples from credit risk, operational risk and market risk have already provided a rather detailed overview of how important the independence of the risk control function is and what tasks such a function would typically be responsible for (reporting, design of the models, backtesting and benchmarking, conducting stress testing, etc.).

The internal audit function

The last piece in the internal governance structure introduced is the internal audit function. The role of internal audit under the Basel II framework is predominantly assessing the independence and the efficiency of the risk control function but also the assessment of the overall compliance with the minimum requirements of the Banking Directive and the Capital Adequacy Directive. In this respect internal audit should regularly report (at least annually) to both the management body and senior management. In order to fulfil this function properly it needs to have access to all relevant internal documents. All recommendations of internal audit should be subject to a formal follow-up procedure in order to ensure their resolution.

By this it should allow the management body to ensure that the quality of the internal controls is both effective and efficient[65].

Internal Audit should also review the adequacy of the IT infrastructure and data maintenance. For institutions using statistical models, this means conducting tests (for example, on specific business units) in order to check data input processes. The audit function should not be involved in day-to-day operations, however, like reviewing each individual rating assignment[66].

Finally, Internal Audit units should always be staffed by individuals possessing the requisite stature, skills, and experience.[67] It is important that they be familiar with the institution's strategy and its processes for identifying, assessing, monitoring, controlling, and mitigating risks.[68].

Summary and outlook

The internal governance structure of a bank is crucial for surviving stress situations or for avoiding them at all. This has been proved once again during the financial crisis, where institutions with a bad internal governance structure were hit the hardest. A crucial part of the internal governance structure is an independent risk control function providing independent reporting to the management body and senior management. Basel II aims at strengthening risk management within the institutions in order to enhance financial stability.

Has Basel II failed because it could not prevent the financial crisis starting in summer 2007? This popular argument cannot really be subscribed to. The moment the crisis evolved Basel II had come into force only for the institutions with a more simple business model using the standardised approaches for credit and operational risk. The more sophisticated IRB and AMA models with their strict requirements concerning an institution's internal governance and the respective Pillar II requirements were coming into force only on 1 January 2008. Both the institutions and the supervisory authorities were therefore still in a preparatory pre-Basel II phase when the crisis got virulent.

With the Banking directive, the Capital Adequacy Directive and the BCBS and CEBS Guidelines complementing these directives the tool box for efficiently supervising an institution and the

[64] CEBS (2008b), p. 44.

[65] CEBS (2006a), p. 18.
[66] CEBS (2006b), p. 109.
[67] CEBS (2006b), p. 137.
[68] CEBS (2006 b), p. 139.

risks it is taking and for enforcing a better quality of risk management has already been established in the years 2006 to 2008. Consequently, there is no real general need for a further set of rules on internal governance like the CEBS high level principles for risk management. It is more the strict application of the already existing framework that matters.

There are two exceptions to this rule, however. One is the forthcoming new rules on compensation schemes, the other considerations on strengthening the role of the Chief Risk Officer. The crisis has shown that independent and swift reporting lines are obviously not enough. It is more the power to make the management body act (or preventing it from acting) following this information that is lacking. The CEBS High-level-principles for risk management therefore correctly stress the necessity to strengthen the role of the CRO. In this respect they reflect industry's best (but not widespread) practice where an authoritative CRO chairs the risk committee(s) that are directly accountable to the management body and – as a member of the management body - reports directly to the CEO[69].

According to the CEBS High-level-principles, that are supposed to be followed by a comprehensive guidebook addressing risk management issues, the Chief Risk Officer should have sufficient independence and seniority to enable him or her to challenge (and potentially veto) the decision-making process of the institution[70]. This seems to be the right way. Only the future, however, will show whether or not this – together with a more strict application of the already existing internal governance requirements and guidelines - will really have helped to avoid further crises.

References

1. Basel Committee on Banking Supervision (BCBS) (1998), Framework for internal control systems in banking organisations, Basel, 1998.
2. Basel Committee on Banking Supervision (BCBS) (2006a), International Convergence of Capital Measurement and Capital Standards. A revised framework, Basel, June 2006.
3. Basel Committee on Banking Supervision (BCBS) (2006b), Enhancing corporate governance for banking organisations, Basel, 2006.
4. Basel Committee on Banking Supervision (BCBS) (2008), Principles for sound liquidity risk management and supervision, Basel, September 2008.
5. Committee of European Banking Supervisors (CEBS) (2006a), Guidelines on the Application of the Supervisory Review Process under Pillar 2 (CP03 revised), http://www.c-ebs.org/getdoc/00ec6db3-bb41-467c-acb9-8e271f617675/GL03.aspx.
6. Committee of European Banking Supervisors (CEBS) (2006b), Guidelines on the implementation, validation and assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches, http://www.c-ebs.org/getdoc/5b3ff026-4232-4644-b593-d652fa6ed1ec/GL10.aspx.
7. Committee of European Banking Supervisors (CEBS) (2008a), Electronic Guidebook, London, March 2008 http://www.c-ebs.org/documents/Publications/Compendium-of-Guidelines/2008-09-03-EGB2.aspx.
8. Committee of European Banking Supervisors (CEBS) (2008b), Second part of CEBS's technical advice to the European Commission on liquidity risk management, London, 18 September 2008.
9. Committee of European Banking Supervisors (CEBS) (2010), High level principles for risk management, London, February 2010, http://www.c-ebs.org/documents/Publications/Stan-dards---Guidelines/2010/Risk-management/HighLevelprinciplesonriskmanagement.aspx.
10. Counterparty risk management group, Containing systemic risk: the road to reform. The report of the CRMPG III, August 2008.
11. European Union (EU) (2006a), Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast), Official journal of the European Union L 177, Brussels 30.6.2006., p. 1-200.
12. European Union (EU) (2006b), Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast), Official journal of the European Union L 177, Brussels 30.6.2006, p. 201-255.
13. European Union (EU) (2009), Directive 2009/111/EC of the European Parliament and of the Council of 16 September 2009 amending Directives 2006/48/EC, 2006/49/EC and 2007/64/EC as regards banks affiliated to central institutions, certain own funds items, large exposures, supervisory arrangements, and crisis management, Official Journal of the European Union, L 302/97, Brussels 17.11.2009, p.97-119.
14. HM Treasury (Walker review), A review of corporate governance in UK banks and other financial industry entities. Final recommendations, London, 26 November 2009.
15. Institute of international Finance (IIF), Final Report of the IIF Committee on Market Best Practices: Prinicples of conduct and best practice recommendations, Washington D.C., July 2008.
16. Jorion, Phillippe, Value-at-risk, 2nd edition, New York, 2001.
17. Kirpatrick, Grant, Corporate Governance lessons from the financial crisis, in: OECD journal: Financial markets trends, Vol. 96, Issue 1, 2009, p.61-87.
18. Mongiardino, Alessandra/Plath, Christian, Risk governance at large banks: Have any lessons been learned?, in: Journal of risk management in financial institutions, Vol.3, Issue 2, 2010, p.116-123.
19. OECD, Principles of corporate governance (2004), Paris 2004.
20. The High-level Group on financial supervision in the EU (The High-level Group), Report, Brussels February 2009.
21. UBS, Shareholder report on UBS's writedowns, Zürich, 18 April 2008.

[69] Mongiardino/Plath (2010), p. 117-120.
[70] CEBS (2010), p. 4-5.