8 April 2009

Consultation paper (CP 24)

High-level principles for risk management

Background and introduction

1. In their declaration of 15 November 2008, the G-20 leaders stated that regulators should "develop enhanced guidance to strengthen institutions' risk management practices, in line with international best practices, and encourage financial firms to re-examine their internal controls and implement strengthened policies for sound risk management"[1].

2. The EU Economic and Financial Committee (EFC) has transposed the G-20 recommendations into its "EU Work Plan Following G-20 Declaration and Action Plan", which repeats the call for CEBS to develop enhanced guidance to strengthen banks' risk management practices, in line with international best practices, and encourage financial firms to re-examine their internal controls and implement strengthened policies for sound risk management.

3. In response to this request, CEBS has conducted an analysis of existing risk management guidelines, with the objective of identifying possible gaps in coverage and other areas where updates to the guidelines would be desirable. The report submitted to the 2009 March meeting of the EFC provided a roadmap for improving existing CEBS guidelines and enhancing their implementation.

4. According to the results of the CEBS analysis, EU and international supervisory bodies have produced a comprehensive set of guidelines covering all major aspects of risk management. However, the coverage of the guidelines is somewhat fragmented, with most guidelines focussing on narrow areas. Furthermore, not all aspects of risk management are covered in CEBS' guidelines. In particular, there are gaps in the areas of: (i) governance and risk culture; (ii) risk appetite and risk tolerance; (iii) the role of the Chief Risk Officer and risk management functions; (iv) risk models and integration of risk management areas; and (v) new product approval policy and process.

[1] G20 declaration of 15 November 2008, http://www.g20.org/Documents/g20_summit_declaration.pdf

5. To overcome this deficiency, CEBS has decided to consolidate all of its principles and guidelines addressing risk management issues in a comprehensive guidebook that covers all aspects of risk management, following the structure of Annex V of the Capital Requirements Directive[2] . Such a consolidation (not to be confused with the simple compilation of texts provided in the current CEBS Electronic Guidebook[3]) will eliminate overlaps and achieve comprehensive coverage of the topic of risk management in one place.

6. To introduce the consolidation of existing principles and guidelines on risk management, CEBS has decided to develop a set of overarching high-level principles on risk management, which would serve as a stand-alone document, but could also be expanded upon in CEBS guidelines on specific topics (in the form of references to existing risk management principles as formulated in CEBS standards and guidelines).

7. The high-level principles proposed in the current paper should be considered both by institutions and supervisors within the supervisory review framework under Pillar 2. In other words, they should be implemented by institutions as part of the ICAAP, and reviewed by supervisors as part of the SREP.

8. The high-level principles for risk management are aimed mainly at large and complex institutions. However, according to the principle of proportionality, they could be adapted to any institution under review, taking into account its size, nature, and complexity[4].

High-level principles for risk management

Governance and risk culture

9. A strong institution-wide risk culture is one of the key elements of effective risk management. One of the prerequisites for creating this risk culture is the establishment of a **comprehensive and independent risk management function under direct responsibility of the senior management**.

10. The management body is responsible for overseeing senior management, and also for establishing sound business practices and strategic planning. It is therefore of the utmost importance that the **management body have a full understanding of the nature of the business and its associated risks**. At least some members of the management body or, where relevant, the audit committee (or equivalent) should carry out an activity in the area

[2] In this paper, all references to the Capital Requirements Directive (CRD) are references to Directive 2006/48/EC.

[3] See http://www.c-ebs.org/Publications/Compendium-of-guidelines.aspx

[4] According to the principle of proportionality, guidelines for institutions and supervisors are to be applied in a proportionate manner to reflect the nature, scale and complexity of the activities of the institutions (see CEBS Guidelines on the Application of the Supervisory Review Process under Pillar 2).

of financial markets or have professional experience directly linked to this type of activity.

11. **Every member of the organisation must be constantly aware of his responsibilities relating to the identification and reporting of risks** and other roles within the organisation and the associated responsibilities to these roles. The risk culture must extend across all of the organisation's units and business lines. Risk policies must be formulated based on a comprehensive view of all business units, and risks must be evaluated not only from the bottom up, but also across individual business lines.

12. Institutions must implement a **consistent risk culture and establish sound risk governance supported by an appropriate communication policy**, all of which must be adapted to the size and complexity of the organisation and the risk profile of the institution or banking group.

Risk appetite and risk tolerance

13. The level of risks that institutions are willing to take is constrained by regulation and supervision, given that the social cost of any institution failure (official support measure) would typically exceed the limited downside risk for institution shareholders and management. Risk tolerance depends not only on intrinsic risk aversion, but also on the current financial situation of the institution and its strategic direction. **Risk tolerance should take all relevant risks into account**, including those arising from off-balance-sheet-transactions. To assure the safety of deposits, this regulatory constraint takes, in particular, the form of capital and liquidity requirements.

14. Institutions express their risk appetite in a variety of forms, including setting a target credit rating or a target rate of return on equity (sometimes, but not always accompanied by a target limit on the variance of that return). It is important **both that institutions set such targets, and that the targets be consistent with one another**[5] as well as consistent with the institution's obligation to maintain the risk of deposits within the constraints implied by capital and liquidity regulation.

15. In setting a risk appetite or risk tolerance level, the institution has to **take all relevant risks to the institution into account**. Models that indicate that the institution stands to earn very high returns on economic capital may in fact point to deficiency in the models (such as failure to take into account all relevant risks) rather than superior strategy or execution on the part of the institution.

16. **The management body and senior management are responsible for setting the institution's risk appetite or risk tolerance** at a level which

[5] For example, supervisors can legitimately question how a bank can simultaneously achieve a high rate of return on equity and a narrow variance around that target rate of return. They may also question how a high target rate of return on equity can be consistent with maintaining a high credit rating throughout the business cycle.

is commensurate with sound operation and the strategic goals of the institution.

17. The **respective roles of the management body and senior management in the oversight of risks should be clearly and explicitly defined**. The management body should be responsible for setting the institution's risk tolerance level, and for reassessing that tolerance level regularly, taking into account the information provided by the risk management function or, where relevant, by the audit committee (or equivalent).

18. **Senior management should be responsible for risk management on a day-to-day basis**, under the oversight of the management body. Because of the volatile nature of the banking business and the economic environment, risk measurement should be constantly reviewed and scrutinised against the institution's strategic goals and risk tolerance. In particular, senior management should ensure that the institution sets trading, credit, liquidity, and other risk limits that are consistent with the institution remaining within its overall risk appetite, even in a stressed economic environment.

The role of Chief Risk Officer and the risk management function

19. The institution should appoint a **person responsible for the risk management function across the entire organisation**, and for coordinating the activities of other units relating to the institution's risk management framework. Normally this person is the Chief Risk Officer (CRO). However, when the institution's characteristics – in particular its size, organisation, and the nature of its activity – do not justify entrusting such responsibility to a specially appointed person, the person responsible for internal control can be made responsible for risk management as well.

20. The **CRO (or equivalent) should have sufficient independence and seniority to enable him to challenge (and potentially veto) the decision-making process of the institution**. His position within the institution should permit him to communicate directly with the executive body concerning adverse developments that may not be consistent with the institution's risk tolerance and business strategy. When the executive body or the management body considers it necessary, the CRO should also report directly to the management body or, where appropriate, to the audit committee (or equivalent).

21. The **CRO should have expertise which matches the institution's risk profile**. He should play a key role in making the management body and senior management to understand the institution's overall risk profile.

22. The **risk management function should also have expertise which matches the institution's risk profile.** It should play a key role in identifying, measuring, and assessing the overall risks faced by the institution. Its responsibilities should include overseeing and approving

internal ratings systems and risk assessment models, and analysing the risks of new products and exceptional transactions.

23. The **risk management function should be actively involved, at an early stage, in the elaboration of the institution's strategy** and decision-making on business activities.

24. Institutions should ensure that the **risk management function is independent from the operational units** whose activities they review. Their position in the organisation should allow them to interact with these units in order to have access to the information necessary for the accomplishment of their mission. However, the risk management function should in all cases be carried out at arm's length from the decision-making function.

25. **The management of risks should not be confined to the risk management function.** It should be a responsibility of management and staff in all business lines, and they should be aware of their accountability in this respect.

26. The **management body and senior management should be responsible for allocating resources to the risk management function** in sufficient amounts and quality to allow it to fulfil its missions. These resources should be consistent with the institution's risk management and strategic objectives. They should include adequate personnel (with sufficient expertise and qualifications), data systems and support, and access to internal and external information deemed necessary to the fulfilment of the risk-management's missions.

Risk models and integration of risk management areas

27. Institutions should **identify and manage all risks** across all business lines at the portfolio and group levels, whatever the nature of the exposure (contractual or not, contingent or not, on- or off-balance sheet).

28. Institutions should **avoid over-reliance on any specific risk methodology or model**. Modelling and risk management techniques should be only one part of the risk management system, and should always be tempered by expert judgment.

29. Institutions should adopt an integrated treatment of risk when they decide to launch new products or activities.

30. **Risk-taking decisions should not only be based on quantitative information or model outputs but should also take into account the practical and conceptual limitations of metrics and models used by a qualitative approach including expert judgment and critical analysis**. Relevant macroeconomic environment trends and data should explicitly be addressed to identify their potential impact on exposures and portfolios. Such assessments should be formally integrated in material risk decisions. In particular, institutions shall bear in mind that the results of stress testing

exercises are highly dependent on the limitations and assumptions of the models, namely the severity and duration of the shock and the underlying risks.

31. **Regular and transparent communication mechanisms should be established** within the organisation, so that the management body, senior management, business lines, the risk management function, and control functions can all share information about risk measurement, analysis, and monitoring.

32. **Internal procedures and information systems should be consistent throughout the institution** and reliable, so that all sources of risks can be identified, measured, and monitored on a consolidated basis, and also, to the extent necessary, by entity, business line, and portfolio.

New product approval policy and process.

33. **Institutions should have in place an internally approved and well-documented "new product approval policy" (NPAP)** which addresses not only the development and approval of entirely new products, but also significant changes in the features of existing products.

34. The new product approval policy should cover all aspects of the decision to enter new markets or deal in new products, including the definition of "new product/market/business" to be used in the organisation, the internal functions involved in the decision (possibly through an ad-hoc committee), and other issues involved in undertaking a new activity (pricing models, P&L, software, back and middle office, risk management tools, etc.).

35. New products, markets, and businesses should be analysed carefully, and the institution should make sure that it possesses adequate internal tools and expertise to understand and monitor the risks associated with them.

36. The risk management function must participate in the process of approving new products or significant changes to existing products. It should also have a clear overview of the roll-out of new products (or significant changes to existing products) across different business lines and portfolios, and should have the power to require that changes to existing products go through the formal NPAP process.