

## **CEBS' Consultation paper (CP 24) High-level principles for risk management**

### **Response of the AMAFI**

1. AMAFI thanks CEBS for providing it with the opportunity to provide its views on the proposed set of overarching high-level principles on risk management.

AMAFI is committed to promoting sound risk management practices in the financial industry. As an illustration, it created at the beginning of the year a working group composed of risk officers and dedicated to the matter of strengthening risk management practices in financial institutions. Since then, the group has been intimately involved in an initiative launched by the French supervisor to enhance regulation in this respect and develop professional best practices.

AMAFI's observations on this set of principles build therefore on the work conducted so far by this working group.



2. As a preamble, it should be stressed that the proposed principles do not give rise to any major observations, as they are generally quite consensual. As experienced in our work with the French supervisor, the difficulties do not lie so much into the high-level principles themselves but rather in the practicalities for national authorities of translating them into regulation.

As a general observation, it is felt that the order in which some of the principles are organised could be adjusted to match better the various sub-sections' titles. In this respect, the following re-ordering could enhance the clarity of the document:

- Move at least the first sentence of §17 and § 18 into 'Governance and culture'.
- Paragraph 11 that deals with risk culture in its first part may be better placed after § 9. The last sentence related to risk policies seems to belong to 'Risk appetite and risk tolerance'
- Paragraph 29 should move to 'New product approval policy and process'

Finally, before commenting on the various subsections, it should be stressed that it is not clear whether the principle of proportionality highlighted in § 8 will be part of the principles themselves – we strongly suggest that it be so, as it is paramount to make the principles adaptable to all financial institutions.

➤ **Governance and risk culture**

3. A strong risk culture is indeed a key element to effective risk management. In AMAFI's view, this culture should be instilled from the very top of the institution, i.e. by the management body. It is nurtured further by dedicated functions such as the risk management one, who makes it live and permeate through the day-to-day activity of the staff but, to complement what is proposed in § 9 of the principles, the most important pre-requisite is first involvement of the senior management. Without it, the risk management function alone would be helpless to establish a truly effective risk culture. We propose to write: *"One of the prerequisites for creating this risk culture is the management body's involvement in instilling this culture. A comprehensive and independent risk management function under direct responsibility of the senior management contributes to this end."*

4. In paragraph 11, the reference in the first sentence to *"other roles within the organisation and the associated responsibilities to these roles"* is not clear.

➤ **Risk appetite and risk tolerance**

5. Paragraph 14 seems limitative in the forms of risk appetite it provides as examples. Another way to express a firm's risk appetite is the use of limits, which is a simple method that many firms of a smaller size use.

6. Paragraph 18 refers to the banking business, putting aside other financial activities conducted by investment firms (in France for example the terms banking would not refer to an investment firms' activities), which should be in scope of these principles (for an example of a regulation common to banking and securities regulators, please refer to the capital requirement directive 2006/49/EC of 14 June 2006 that applies both to investment firms and credit institutions).

This paragraph also refers to senior management's responsibility for *"risk management on a day-to-day basis, under the oversight of the management body"*. In AMAFI's view, if the terms *"senior managers"* refer to executives of the institution who are not part of the executive body, the oversight should be carried out by the executive body; but such a statement would not add value as it would only be a reflection of the current organisation of institutions. If *"senior management"* refers to the executive body, it is indeed responsible for risk management but the addition of *"on a day-to-day basis"* seems excessive, as the day-to-day risk management generally belongs to a lower level of management. In AMAFI's opinion, one should read: *"The executive body should be responsible for risk management"*. Incidentally, it may be worth explaining the meaning of the terms *"senior management"*, frequently used in the document, in contrast with the management body and executive body (see for example § 26, where a similar issue arises).

➤ **The role of Chief Risk Officer and the risk management function**

7. The responsibility of the CRO for risk management across the entire organisation raises the issue of defining what is meant by entire organisation, i.e. should the businesses that are not supervised by the authority in charge of banking institutions (e.g. asset management business in France is not under the supervision of the banking authority) be included as well providing they are create risks for the organisation as a whole?

Additionally, the designation of a CRO for the entire organisation does not consider the situation where the subsidiaries of the organisation located abroad are themselves subject to the obligation of designating a CRO locally, as may be imposed by the host supervisor. There could therefore be a conflict between national obligations, for which the designation of a CRO at the group level would not be sufficient, resulting in the need to articulate the responsibilities of several CROs, at different levels of the organisation, some of them encompassing a narrower scope. This also raises the question of the most appropriate organisation for firms, especially in terms of choosing between branches and subsidiaries, the first ones being subject to the home country's supervisor, the second to the host country's one.

8. Paragraph 20 indicates that the CRO could potentially veto the decision-making process of the institution. Apart from the fact that it is not so much the process that should be challenged but the decisions themselves, this statement raises two points:

- First, the CRO's veto is only worth the value the management body is willing to confer to it, i.e. it is important to note that the ultimate decision belongs to the management body. As a result, when the CRO vetoes a decision, this is only so until the issue is escalated to the proper management level for ultimate decision.
- Second, his/her ability to challenge a decision or a possible development being contemplated hinges on his/her access to this type of information, i.e. the principles should state that the CRO is provided by the management (or executive) body with the information necessary to perform his/her role (this idea is under lied in § 23 but not explicitly expressed).

An alternative wording could be:

***“The CRO (or equivalent) should have sufficient independence and seniority **and should be provided access to the necessary information by the executive body** to enable him to challenge (and potentially veto) the **decisions** of the institution. If the CRO's decision is challenged, a process exists to escalate the issue to the management body for ultimate decision”***

9. The second sentence assumes that the CRO assesses adverse developments in respect of the “*institution's risk tolerance and business strategy*”. In AMAFI's view, the CRO's role is not to ensure consistency with the business strategy but rather to check consistency with the risk tolerance set for the institution. Developments' consistency with the strategy is a matter for the management body. However, the principles should state that the business strategy itself is set by the management body considering the risk tolerance of the firm.

10. The last sentence of the paragraph states that “*when the executive body or the management body considers it necessary, the CRO should also report directly to the management body*” but there is no mention of the reporting line of the CRO in the previous statements of this section (it is only indicated that the CRO communicates “*directly with the executive body*”). Therefore a principle should be added to state that “*the CRO should report directly to the executive body*”.

11. Paragraph 21 states that the CRO plays a key role in making “*the management body and senior management understand the institution's overall risk profile*”. However, there is no direct link established between the CRO and the management body, unless the latter requests it (see § 20). It should therefore be replaced with “*executive body*” or the link should be defined.