Comments on CEBS Consultation Paper CP 24 ("high-level principles for risk management")

Background and introduction

….omissis…

General Comments

AIFIRM welcomes CEBS CP24 proposal as a sign understanding of the relevance and importance in today context to set an effective risk governance in order to restore trust into the banking sector and the financial industry.

1. AIFIRM considers that, despite progresses in recent years, risk management techniques have not yet reached a satisfactory comprehensive framework. More effort is needed to define mission, systems and requisites, as already done by BCBS and IASB in the field of *valuation*, similarly touched by recent crisis' events.

2. The CP24 document is devoted to Risk Governance principles. To fulfill these principles, an adequate risk management profession's definition is needed, to give awareness, transparency and clarity on duties, roles and profiles. It has to be noted that professions like Accountants, Auditors, Analysts e Corporate Lawyers are far better defined and rooted in corporate organization and profiles.

AIFIRM proposes to create a common working group among Risk Manager Associations and CEBS, to go more in depth in these topics and to better define a risk management code of conduct, giving reference points to CROs, Risk Managers and practitioners in Europe. The aim would be to set Standards of Best Practice & Conduct, to properly define the profession applied to the financial industry.

Appropriate risk management can often produce results that are not popular with other corporate interested parties. Proper risk assessment can also require adaptation of established methodologies and new approaches, due to any number of the factors involved in risk assessment.

The fact that the risk professional may be a bearer of bad news, and must exercise personal judgment in producing and interpreting results, requires the highest standard of personal and professional conduct.

Standards must promote the highest levels of conduct and provide direction and support for the risk management profession.

We could cite, for instance, some principles

Basic Knowledge

The risk manager profile has to respect a level of competences to fulfill the risk assessment/management work at hand. The risk manager moreover must be well versed in all rules and regulations applicable to the processing and presentation of risk assessments and must be familiar with current generally accepted risk practices, noting any relevant departure from generally accepted risk practices. Disseminating improvements in risk management methods and/or theory to the widest professional audience is essential in the risk manager profession, as well as the openness to validation by peers, internal/external to the organisation.

Honesty and Integrity

The Risk Manager must act with diligence, honesty and integrity, must not engage, and should discourage from engaging in, activities that are intended to deceive others. The member should avoid any actions that will reflect badly on the risk management profession. The Risk manager should collect, analyze and disseminate risk information with the highest level of professional objectivity, and endeavour to work in manner that would be deemed appropriate by an independent properly qualified risk practitioner.

Specific Comments

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****.*

It needs to consider that risk management is primarely managing and not only measuring risks. In this perspective an isolation of risk management function in a line only reporting to the Board and not to the executives could be penalizing because of the lack of professional support to management (i.e. pricing, valuing, hedging and monitoring risk at operations level).

AIFIRM agrees with this principle. Risk Management should be a process as well than a role in the financial institution; in order to do this it needs to be implemented a strong risk culture.

It may be the case for Regulators to include into the SREP a kind of assessment of the presence and the spreadness of such a culture. In particular the level of

risk knowledge should be assessed into the Senior Management body as correctly covered by the point n.10

…Omissis…

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***[1] *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.*

Regarding this point, it is essential:

- to assure coherence to the risk appetite definition,
- to monitor & control risk profile observance in day by day decisions, also implementing adequate procedures in pricing, administration, accounting, incentives & responsibilities, MIS contents,
- to define risks that should be avoided at any cost.

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

[1] 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.

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 Risk Management is highly relevant in this view. Senior management has to be aware of risk but cannot be as competent as the risk manager are in methods and models. Risk Managers behavior in terms of Transparency, Honesty, Integrity and Accountability are principles to be defined and applied, to give thickness to proposed CEBS risk governance principles. In particular independence and possibility to escalate corporate powers, to reach a correct risk representation to the top management, are essential.

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.*

AIFIRM's opinion is that internal control has to be set absolutely indipendent from the management of the business and from any decision taken by line manager. So we think that, in small institution, Risk Management function could be accomplished by CFOs or Head of Planning and Budgeting but not by Internal Auditor or third level controls.

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).*

Some associations spoke about a sort of Hippocrates Oath for Risk Managers. Without arriving to this point, a strong commitment is needed for CROs to assure independency, autonomy, transparency of risk profiles and decisions.

…Omissis…