16 February 2010

Feedback to the consultation on CEBS's High level principles for risk management (CP 24)

1. On 8 April 2009, CEBS submitted for public consultation **its High level principles for risk management.** The consultation period ended on 10 July 2009. Nine written responses were received[1]. Due to the late submission of one comment, only eight comments have been taken into account in the feedback table. However, those comments have been much in line with other comments received, so that this had no significant impact on the review of the consultation paper.

2. This paper presents a summary of the key points arising from the consultation and the changes made to address them.

3. Respondents welcomed and largely supported the proposed guidelines and considered them to be a good basis for the development of comprehensive risk management principles. However, some suggestions on content and wording were received.

4. Most respondents said they would welcome the development of more detailed guidelines on specific topics as more detail was needed to facilitate the implementation of the Guidelines. The implementation of risk management models was a key issue. It was also stressed that the guidelines should be aligned with principles set by other international bodies.

5. Respondents appreciated that the principle of proportionality is considered to be an overarching principle which will provide sufficient flexibility.

6. The Guidelines have been revised on the basis of the comments received. A few suggestions have not been taken into account within the High-level principles as they seek a level of detail which was not intended to be provided by the guidelines under consultation. However, those comments may be taken into account in the development of a comprehensive set of guidelines

[1] The responses to CP24 are published on the CEBS public website under: http://www.c-ebs.org/getdoc/511d2592-174a-40d7-9010-dd798c3f7c12/Responses-to-CP24.aspx

7. A feedback table is provided in the annex which gives a detailed description of the comments received and CEBS´s responses to them.

Annex

Feedback table on CP24: analysis of the public responses and suggested amendments

CP24	Summary of comments received	CEBS's response	Amendments to the proposals set out in CP24
High-level principles for risk management			
Section: Background and introduction			
Paragraph 5	It would be helpful if CEBS could outline the next steps in creating a comprehensive guidebook and who is intended to take action on them.	CEBS has mandated a working group to revise the guidelines on internal governance and risk management, taking into account the developments in the international fora (e.g. Basel Committee). CEBS guidelines are primarily directed at supervisory authorities who will implement them in their regulation or supervisory processes. One objective is to achieve a harmonised regulatory framework, another is to achieve sound governance and risk management standards. The guidelines are also aimed at institutions, without being legally binding. However, with the setting up of the European Banking Authority (EBA) in 2011, it will develop legally binding standards in some areas.	No change
Paragraphs 7, 11, 27, 32	In paragraph 7 it should be specified that these requirements apply only to the relevant and	The scope of the risks to be included in the ICAAP and the SREP is part of guidelines and was	No change in paragraph 7;

	material risks of an institution. Reference to the 'relevant risks' is already made in paragraphs 13 and 15. An explicit reference to the 'relevance' and 'materiality' of risks is particularly important in the context of the requirements on governance (paragraph 11); risk identification through models (paragraph 27) and risk management processes (paragraph 32).	therefore not defined within the introductory chapter. All relevant risks must be taken into account. To assess the relevance of a risk it has to be identified first. Only after this can it be judged not to be relevant. Comments on paragraphs 11, 27 and 32 were accommodated by adding "relevant" to the word "risk".	paragraphs 11, 27 and 32 amended and renumbered.
General comment	Respondents recognised that the High-level-principles only cover some aspects of risk management and suggested clarifying that it was no intended to provide a comprehensive set of guidelines. In addition some benefit was seen in being more concrete in some areas (e.g. responsibilities for all staff, general approach to risk management, specific role of independent risk control functions, responsibilities of risk management oversight bodies).	It was not intended that the High-level-principles include a detailed and comprehensive set of guidelines. Paragraphs 4-6 already describe the purpose of the guidelines sufficiently. More work in this area will be done in the future.	No change
Section: Governance and risk culture			
Paragraph 8	Most respondents explicitly acknowledged the principle of proportionality. One respondent suggested explicitly recognising that the principle of proportionality applies to the firm's overall approach to risk management and the role of the risk control functions(s) which should reflect the risk profile and culture of an institution.	The principle of proportionality allows for flexibility in the implementation of the guidelines, because a "one size fits all" approach to supervisory guidelines is not possible. However, all institutions must manage their risks appropriately. This includes sufficient challenge to decisions by the risk control function, which is one part of creating a risk culture. A culture which accepts a high level of risk (independent from how it can be measured) cannot be a reason for reducing the level of risk control measures.	No change

Paragraph 9	Respondents asked for clarification of the meaning of "comprehensive" and suggested that this means risk control functions which cover all the risk types, business lines and material risks to which the institution is exposed. Further, as risk management in a firm may be organised across different functions reflecting different risk types, risk control functions should be referred to in the plural.	While the suggested definition of "comprehensive" seems to be helpful to stress that a holistic risk management approach is a key issue, the inclusion of different risk control functions without having additional guidelines on them could have lead to misinterpretations. Especially in groups, different organisational units may exist for risk management purposes, with one of them responsible for aggregating the risks into a holistic view of all relevant risks. The whole collection of functions/units is considered to be the risk management function.	Paragraph 9 amended
Paragraphs 9-12	Respondents suggested deleting the term "risk culture". They perceived "that it is problematic to raise it to the rank of principle, as the risk culture is … the result of the establishment of adequate management and reporting processes, and thereby part of the 'governance' issue." The supervisory assessment of the internal risk culture of an institution may be not possible as well.	One of the objectives of the guideline is to foster the creation of a risk culture within financial institutions. The guidelines set out in enough detail elements which need to be implemented to create a risk culture. This may also enable supervisors to check if an institution has implemented sufficient measures to achieve this high level objective.	No change
Paragraph 10	Respondents raised the issue that there are various levels of understanding required within the management body. While it should be expected that the Chief Risk Officer (CRO) and Finance Director have a full understanding of the technicalities in the area of risk management, it should suffice for other members of the management body to have a more general understanding of the risk factors and models. Therefore it was suggested to replace "full understanding" with "level of understanding commensurate with their responsibilities". It was also suggested to amend the paragraph to align the required experience of the management with	The management body collectively has to have a full understanding of the nature of the business and its associated risks. However, individual members need a level of understanding commensurate with their responsibilities. This includes an adequate understanding of those areas of business undertaken by the institution for which they are not directly accountable.	Paragraph 10 amended

	business needs in order to account better for the needs of specialised institutions.		
Paragraph 10	The meaning of “management body” as opposed to “senior management” should be clarified.	‘Management body’ is defined in Article 11 of the CRD and should be understood to embrace different structures, such as unitary and dual board structures. The management body represents the top management level of an institution and senior management (which is not defined in the CRD) should be understood to represent the level of management below the management body. (see also para. 413 of CEBS Guidelines on Validation, http://www.c-ebs.org/getdoc/5b3ff026-4232-4644-b593-d652fa6ed1ec/GL10.aspx)	No change
Paragraph 11	The Consultation Paper seems overly ambitious where it states that "Every member of the organisation must be constantly aware of his responsibilities relating to the identification and reporting of risks." It was suggested that it should be made clear that every relevant member of the organisation must be aware of his responsibilities in this respect.	It was intended to stress that building up risk awareness and risk identification is not just a one off procedure and that the tasks to be performed with regard to risk management are recurring ones. The principle has been clarified.	Paragraph 11 amended and new paragraph 13 added, subsequent paragraphs renumbered
Paragraph 11	Each team member’s responsibilities for the identification and reporting of risks should be documented in writing and shared. Training must be provided on all relevant areas of risk on an on-going basis, including on the identification and reporting of risks. Risk policy must be updated regularly and changes should be communicated throughout the organization.	All significant governance arrangements must be documented and updated appropriately. This has been added into the guidelines as a general principle.	New paragraph 13 added

Paragraph 11 and General comment	Respondents asked CEBS to include explicitly non-financial risks in the principles (e.g. reputational risk, compliance with codes of conduct, information security), as those risks need to be taken into account as well as financial risks. The proposed guidelines seemed only to deal with financial risks.	Institutions need to take into account all relevant risks. However, a strict differentiation of those risks would need clear definitions. As most of the examples provided could cause losses to an institution they could be considered to be financial risks. However reputational risks in particular can be relevant and will be mentioned in the guidelines.	Paragraph 11 amended
Par 12	It was proposed to replace the paragraph with the following language: "Institutions must implement consistent risk control standards and principles with sound governance arrangements. These standards and principles, and the governance structure should be communicated appropriately."	One of the objectives of the guideline is to foster the creation of a risk culture within financial institutions. This concept includes a much wider scope than the proposed redrafting, as it also including strategies, business line activities and, not least, sufficient risk awareness across the institution.	No change
General comment	Respondents were afraid that the notions of management body and senior management may be interpreted in different ways. A non-executive board of directors should approve and not set the risk tolerance which is defined by the executive management. It should be stressed that risk management is firstly a responsibility of the executive and senior management.	The management body covers both the management function and the supervisory function. Both functions are crucial to achieve sound risk management practices. For the purpose of the high level principles it was not intended to specify the purpose of the different functions of the management body. However, other guidelines (Guidelines on Validation and Guidelines on Supervisory Review Process) do so. The revision of guidelines on the supervisory review process, encompassing guidelines on internal governance, will be subject to future CEBS work. .	No change
Section: Risk appetite and risk tolerance			
Paragraph 13	Respondents wished to delete "The level of risk that institutions are willing to take is constrained by regulation and supervision, given that the	The sentence substantiates the necessity for regulatory restrictions with regard to institutions' risk appetite, reflecting the impact the financial	No change

	social cost of any institution failure (official support measure) would typically exceed the limited downside risk for institution shareholders and management' as this is superfluous."	crisis has had on the economy. This helps to stress the importance of setting an appropriate risk appetite.	
Paragraphs 13 and 15	One respondent suggested consolidating paragraphs 13-15 and differentiating between "risk tolerance" for risk factors that a firm could never hope to eliminate entirely but must manage down to an acceptable level (e.g. operational risk) and "risk appetite" for risks which are actively taken, typically risks that it believes will ultimately be of a profitable nature for it.	While there are slight differences in the conception of the terms, a strict distinction between them will not add additional value to the principles proposed. The level of risks both actively taken and acquired without the intention of generating a return on the specific risk must be considered when setting a risk appetite or risk tolerance level. When doing business, all relevant risks, independent of their origin have to be taken into account.	No change
Paragraphs 13 and 15	'Risk appetite' and 'risk tolerance' are used by CEBS as being largely synonymous in practice. The requirement in paragraph 15 asking an institution to take into account all relevant risks when setting its risk appetite or risk tolerance level overlaps with the requirements in paragraph 13. The duplication should be deleted as well as the last sentence of paragraph 13.	The overlap between the paragraphs will be removed from the text, while the objective of the protection of deposits is kept in para. 13.	Paragraphs 13 and 15 amended and renumbered
Paragraphs 13-16	Risk tolerances should also be established in writing and communicated clearly throughout the organization.	The term "setting" of risk tolerances implies their documentation and communication to relevant staff. However, the proposed change is included in the guidelines as a general principle.	New paragraph 13 included
Paragraph 14	Beside some minor drafting suggestions the inclusion of the following was proposed: "Further, the targets that define risk appetite should be set within a framework that is part of an explicitly stated, coherent strategy. This strategy should describe what the firm seeks to achieve, by region and business line, and outline the institution's risk appetite to include target	A link between strategic planning and risk management was already included within paragraphs 10 and 13 of the guidelines. The suggestion is acknowledged, but it was not intended to provide a detailed guideline on strategies within the "High-Level-Principles for Risk Management".	No change

	metrics for capital usage and return on capital, aligned to those objectives."		
Paragraph 15	It was suggested deleting the second sentence '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' should be deleted." Other principles in the document also address the issue of over-reliance on models (see for instance paragraph 28).	The guidelines with regard to models have been summarised in paragraph 28. The sentence proposed for deletion has been kept. Supervisors are aware that a model signalling overly high returns on economic capital may, but not necessarily, point to model deficiencies.	Paragraph 15 amended and renumbered and the second sentence of paragraph 15 moved to new paragraph 30
Paragraph 17	It was suggested replacing "setting" with "approving" as the management body does not perform the technical process of analysing and determining the risk tolerance.	The term "setting" does not necessarily include the technical steps for determining a possible risk appetite. However, the responsibilities of the management body go beyond the mere approving of suggested figures. As the text already states, the management body takes into account the information provided by the risk management function. An example of this information has been included for clarification.	Paragraph 17 amended and renumbered
Paragraph 18	Expecting a 'constant' review is not realistic. The wording should be revised. Senior management have the day-to-day responsibility for risk management. The actual oversight should occur "as appropriate and proportional to the risk profile and commensurate with the rate of change of the underlying risk exposure." Senior management should ensure that limits are set consistent with the goals of the institution.	The comment has been accommodated and the wording changed ("regularly reviewed"). While the principle of proportionality applies anyway, the following sentence was added for clarification on on-going compliance with the risk appetite, "To this end institutions must have processes in place to ensure risks are kept within the limits and overall limits remain consistent with the overall risk appetite."	Paragraph 18 changed and renumbered
General comment	There needs also to be a periodic independent audit of the entire risk management framework. Such a review can/should be performed by the	All relevant aspects of an institution should be subject to independent review. For the sake of completeness this has been included in the	New paragraph 13 included

	internal audit department.	guidelines.	
Section: The role of the CRO and the risk management function			
Paragraph 19.	Respondents asked for more detailed guidelines on, or examples of, when it is appropriate to not have a separate Chief Risk Officer.	The use of "High-Level Principles" was intended to avoid the need for being too detailed on specific issues at this stage. The development of more detailed guidelines on internal governance is already included in CEBS's work program.	No change
Paragraphs 20 and 21	The language should be gender neutral.	The comment has been accommodated	Paragraphs 20 and 21 amended and renumbered
Paragraph 20	The reference to a potential veto right could be misleading and should be removed. The authority of the CRO to challenge should be such that even the Chief Executive Officer would hesitate to override his position.	A potential veto right would strengthen the position of the CRO, CEBS therefore sees no need to delete the reference mentioned. The competence and role of the CRO is already described within the guideline (e.g. Paragraph 21).	No change
Paragraph 21	It was suggested replacing "expertise" with "relevant skills and experience", "matches" with "relevant and appropriate" and "making" with "leading" or "bringing" to make clear that there is a learning process involved.	The content is not changed by the suggestions, the section was redrafted to clarify the language.	Paragraph 21 amended and renumbered
Paragraphs 21 and 22	It was suggested that paragraphs 21 and 22 are brought together as the same principle applies to the CRO and the risk management function, while the tasks to be performed should be described separately.	Separate paragraphs for the CRO and the risk management function ensure an appropriate level of granularity of the guidelines.	No change

Paragraph 22	It was suggested adding that the risk function should have a leading role in ensuring adequate understanding of risk, as necessary and appropriate, throughout the organisation.	The understanding of risk is needed at both the management level and business line level. The role of the internal control functions will be part of more detailed guidelines based on the Guidelines on Supervisory Review Process.	No change
Paragraph 25	Para. 11 should be replaced by Para. 25.	Due to other changes to Paragraph 11 and the new Paragraph 13 this comment was not longer applicable. Paragraph 25 was kept in its original place.	Paragraph 11 has been redrafted and Paragraph 13 added.
Paragraph 26	The principle should be amended to say that the management body or senior management should ensure that sufficient resources are allocated.	The comment has been accommodated.	Paragraph 26 amended and renumbered
Section: Risk models and the integration of risk management areas			
Paragraph 27	It was suggested moving this paragraph to paragraphs 13 or 15.	While paragraphs 13-18 deal with the "risk appetite and risk tolerance", paragraphs 27-32 are about "risk models and integration of risk management areas." Of course there is a lot of common ground between the two areas but the structure chosen seems appropriate.	No change
Paragraphs 28 and 30	It was suggested merging Paras. 28 and 30 as they are similar.	The document was restructured accordingly. However, two separate paragraphs were kept.	Paragraph 29 moved after Para. 30 and renumbered
Paragraph 29.	Respondents commented that the integrated treatment of risk must cover both old and new products but the guidelines only seem to focus on risk treatments for new products/services.	The general requirement to manage all risks is already included in paragraph 28 (paragraph 27 of the CP). As new products may create significant new risk exposures, the new product approval process and related policies are the chief contols to ensure that possible changes are	Paragraph 29 amended and renumbered

		identified in the risk profile and in the scope of the risk appetite of the institution.	
Paragraph 29	Respondents understood the wording 'integrated treatment of risk' in paragraph 29 in the sense that an institution has a broad overview of the relevant risks related to the launch of new products or activities. This does not mean however that the corresponding risks should be integrated into a risk model. This principle would better fit under the last section on 'New product approval policy and process' (after paragraph 35).	Risk management must take all relevant risks into account in an integrated way. This also applies to new products and activities and is independent of the use of models or different assessment methodologies. New products must be included in those processes. Paragraph 35 already includes the requirement to have adequate tools in place.	Paragraph 29 amended and renumbered
Paragraph 30	Respondents commented that within the decision making process it must be possible to differentiate between decisions taken in the course of standard business and other segments, as profitable standard business requires standardised processes to a great extent. Expert judgment and the like can only be used here at the aggregated level and not in every individual decision. The Consultation Paper contains the phrase "such assessments should be formally integrated in material risk decisions". Documenting a macro-economic assessment for each and every material transaction is unrealistic. Hence, the scope of this requirement can only extend to fundamental decisions which affect the overall strategic alignment; it should not apply to individual risk decisions within the meaning of business decisions.	As the principle of proportionality has to be applied, there is room for simpler processes for standard business. However, the principle that quantitative information has to go together with a qualitative approach applies. The guideline does not require a separate model or expert judgement for every single contract, the term risk–taking decision needs to be considered on a broader basis and in the overall context of the high level principles. Macroeconomic analysis can be done at exposure or portfolio level, as already mentioned in the guideline.	No change
Paragraph 31	Paragraph 31 largely corresponds to the requirements in paragraphs 11 and 12. Therefore, respondents recommended that the principle be moved into the section on governance.	Para. 31 is focussed on the communication process with regard to risk management information. This naturally encompasses some governance aspects. Considering that the focus is on the process, the structure of the paper was not changed.	No change

Paragraph 32	Respondents raised the issue that organising risk management on a consolidated basis is currently facing operational difficulties because of existing differences in Member States' legislation (existence of national options and discretions) and interpretation. Banks' risk management practices will therefore benefit from increasing convergence.	The comment is appreciated. The harmonisation of the supervisory framework within the European Union is one of the objectives of CEBS and the future EBA.	No change
Paragraph 32	The expression "on a consolidated basis" is misleading as it cannot mean that the identification, measurement and monitoring of risks has to take place on a consolidated data basis, i.e. under consideration of intra-group consolidation. It would be better to use "on a common basis" or "on an aggregated basis".	A consolidated risk management approach may be desirable in some areas but on a holistic basis not achievable. The drafting suggestion has been accommodated.	Paragraph 32 amended and renumbered
Paragraph 32	It was suggested that the procedures and information systems should be "coherent" instead of "consistent." It was believed that this requirement should be proportionate to the cost of implementing this in practice and the relevance and materiality of the risk and so the risk control benefit derived from doing it.	Institutions must be able to have a holistic view of their risks. For this purpose institutions must be able to aggregate the information. The guideline does not necessarily aim at a fully automated process. However information should be sufficiently consistent that it allows the creation of a holistic view.	No change
Section: New product approval policy and process			
Paragraphs 33-36	Paragraphs 33, 34 and 36 should be consolidated, paragraph 35 can be deleted. For new product approval and policy it is more effective to involve specialists/line of business control functions in the discussion.	The granularity of the paragraphs helps with understanding the different aspects of the new product approval policy and process. The risk management function must be included in the process. However, this does not mean that experts from the business control functions should not be included as well.	No change