

CEBS

Via email cp35@c-ebs.org

CC: Mr. Arnoud Vossen

Date March 31, 2010

Reference BR1109

Subject: NVB Reaction to CEBS consultation on the management of operational risks in market related activities

Dear Sir, Madam,

The Netherlands Bankers' Association¹ (NVB) welcomes the opportunity to comment on CEBS Consultative paper 35 on the management of operational risks in market related activities. Recent history has shown that staying *in control* in a trading environment is very important. Given this background we understand that CEBS is looking to clarify the expectations in this area. In our view, a lot of the suggested guidelines are already in place at banks in the Netherlands, in areas such as procedures, reporting of policy deviations, the monitoring of (accounting) margins, performing reconciliations, having gardening leave requirements in place, applying changes to systems and real time reporting.

In our view, a key distinction is missing from the consultative paper. By this we mean the three lines of defence that should be set up. Next to the fact that the front office – which is responsible for the deals they do and the associated risks - should execute trades according to the policies and mandates. The lines of defence are:

1. Risk Control; the first line of defence
2. Risk Management, Compliance and Finance (product control); the second line of defence
3. Audit; the third line of defence

The role of risk control could be reflected better in the consultative paper. Where appropriate we will mention this in the detailed remarks. The same goes for the product approval process, which is only mentioned indirectly in the consultative paper.

¹ The Nederlandse Vereniging van Banken (NVB) is the representative voice of the Dutch banking community with over 90 member firms, large and small, domestic and international, carrying out business in the Dutch market and overseas. The NVB strives towards a strong, healthy and internationally competitive banking industry in the Netherlands, whilst working towards wider single market aims in Europe.

Next to this, we do not recognise the statement that is made at the end of paragraph two: *'Institutions have focused their attention on market risk and, as a result, have overlooked the importance of operational risks.'* This statement is not recognized by our member banks and does not take on an objective view of what actually happened in practice.

We also note that a large number of guidelines is put forward in this paper. Given the diversity of market related activities, not all requirements will be equally relevant to all banks. We therefore suggest to split the requirements between key and optional guidelines in order to give banks the opportunity to focus on the most important issues that arise from their specific business model. The objective should be to give banks guidance that will help implement risk management in a structured way, rather than implementing a patchwork of regulations. Wordings like 'minimum requirement' could give an incorrect impression of what CEBS is trying to achieve.

This concludes the main items I like to share with you. In case you have any questions or remarks, please feel free to contact me at your convenience. In the appendix you will find a number of detailed remarks.

Kind regards,



Onno Steins
Advisor Risk Management

Appendix – Detailed remarks

Paragraph 3 mentions that *‘Past and recent cases show that when institutions do not adhere to basic principles of sound internal governance, the severity of operational risk events in market-related activities can be very high, jeopardising the institution’s earnings, the existence of the particular business area or even the existence of the whole institution. As an example, the failure of internal governance mechanisms, at multiple levels, was the main cause of the rogue trading event discovered at SocGen in early 2008.’* Although the governance and operational risk events are mentioned, these are not specified. It would be good if CEBS could elaborate this text.

Regarding paragraph 11, where a number of committees is mentioned, we note that in order for attendance by operational risk management to add value, the risk management representative should have specific product knowledge and should also have the power to reverse trades.

Paragraph 12 *‘The organization structure should guarantee adequate segregation of duties between the front office and the functions in charge of supporting, verifying and monitoring transactions (e.g. back office, middle office, finance, risk management, compliance and internal audit, hereafter called “control functions”). Within each function it should be ensured that, in handling business transactions, activities which are mutually incompatible are carried out by different persons.’* is an example where the various elements of the risk management organisation could have been described in more detail, resulting in clearer picture. Despite the fact that a number of disciplines are mentioned, their tasks are not described and the three lines of defence are not mentioned either. The interactions between commerce and risk are also not properly reflected. We therefore request CEBS to provide additional guidance on this subject.

Principle 2 *‘The management body should promote a front office culture designed to mitigate operational risks in market-related activities.’* contains a number of general highlights that could be made more specific, for instance by including the possibilities for escalation that can be used to remedy adverse developments.

Paragraph 14 *‘High professional standards should be fostered in the front office, for example by issuing a code of conduct for relations between traders and their counterparts.’* does not mention taking responsibility for risks that are taken and the role of the control- and monitoring function. The definition of risk appetite, violation escalation procedures and the governance structure are not included. It could be beneficial to add these items to this paragraph in order to increase clarity as to which elements are meant. The additions should be examples, so that it enables banks to apply the requirements based on their requirements, which result from their individual business model. It would be good if the product approval process and the layers of defence were reflected as well.

Paragraph 15 *‘Appropriate policies and procedures relating to leave requirements and staff movements should be developed, implemented and regularly monitored. In particular: –a policy establishing at least two consecutive weeks’ leave for traders (via a vacation or “desk holiday”) represents sound practice, so that traders are physically unable to mark or value their own books, this responsibility being carried out by a different person during those periods; and –staff movements between front, middle and back-office and IT should be subject to close monitoring, especially if they occur within the same activity or product line.’* puts a lot of emphasis on prevention, but the detection of unwanted developments (done by the second line of defence) is hardly mentioned. The most important thing is that there is a complete monitoring process. In this regard, having a back testing requirement for reported incidents and outstanding risk events could be helpful.

Principle 3, point 18 *‘senior management should ensure that the use of technical accounts (e.g. suspense accounts) is understood by middle and back offices and challenged when used*

inappropriately by the front office. Any suspicious activity across these accounts should be escalated to, and acted on, by senior management. does not explicitly mention the systemic analysis of suspense accounts, even though the analysis of the nature of the positions in the suspense accounts and the detection of undesired developments are important processes. The signalling function of reports is also not mentioned.

There is a lot of emphasis on hiring the right people (for instance paragraph 17), but the monitoring of employee conduct is not mentioned. The latter is important in insuring that employees comply with company policies in their daily work. Examples of monitoring to ensure compliance are the analysis and processing of positions in systems, especially exotics. The creation of transparency and the mitigation of risks are also important. The role of middle- and back office in these processes should receive more attention in the consultative paper. Employees that work in these departments should understand what traders should do to stay in control. We are pleased to see that the importance of having enough knowledge and skills in these departments is recognized in the consultative paper.

Regarding point 19 *'Consideration should be given to the possibility of introducing incentive mechanisms at the level of the control functions to ensure that the oversight of traders' activities is promoted and rewarded. In particular, remuneration of personnel in control functions should reflect the risk-reducing role that they fulfil and, more generally, be based on different drivers from those used for traders' remuneration so as to avoid commonalities of interests and scope.'*, we agree that both the trader and the risk controller should have a common goal; do business with less (little) operational risk. However, we doubt the practical relevance of this point.

Principle 5 *'The fight against fraudulent behaviour in market-related activities should be a pivotal element of internal controls and reporting systems.'* Looking at the objective of this principle, we feel it would be better placed under the section that discusses the internal controls. The principle itself is very important; however there is no reference to the actual processes. We feel it could be beneficial to add these. If processes are not in control, there is an increased chance that operational issues will occur. Thinking along the lines of 'processing value chains' is clearly reflected. Information security may also be an issue.

In principle 6 *'Traders should initiate transactions only when these are compliant with their set terms of reference. Minimum standards for the initiation and conclusion of transactions should be followed.'* an indirect reference is made to the product approval process.

Principle 7 *'Documentation requirements for trading activities should be properly defined. Legal enforceability of the contracts should be assured.'* does not mention any of the other requirements, such as IFRS, SOX and MIFID. These requirements are actually the terms of reference. We request CEBS to make the documentation requirements more specific.

Principle 9 *'Each cash flow associated with a transaction should be clearly recorded in the institution's accounting system, with a documented audit trail.'* Although we agree with principle nine, we request CEBS to make this principle clearer, by adding the various lines of defence. Especially the accounting treatment of exotics would be a good example. The control systems and the governance structure should also be a part of the 'operational risk value chain'.

Paragraph 37 *'Extended audit trails to identify the transaction from the point of origin by each trader is necessary for the institution's systematic ex-post control and reconciliation, both by internal controllers and external auditors, of the operations carried out.'* mentions two functions that are part of the second line of defence. A holistic approach of the processing value chain is of the utmost importance.

With regard to principle 10 *'Institutions should ensure that they have an appropriate framework of controls and procedures applicable to the relationships between traders and their market counterparts.'* we would like to suggest rephrasing it to *'Institutions should ensure that they have an appropriate framework of internal control around the relationships between traders and their market counterparts.'*

Principle 15 *'Information systems in the trading area should be appropriately designed and implemented so as to guarantee a high level of protection in market-related activities.'* does not mention anything about system maintenance. In our view this could be relevant.