# ZENTRALER KREDITAUSSCHUSS

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN


Via e-mail: baselcommittee@bis.org

Basel Committee on Banking Supervision
Bank for International Settlements
Centralbahnplatz 2
4002 Basel
Switzerland

25 February 2011
Burgstrasse 28
AZ ZKA: BASEL
AZ BdB: C 17 - Sz/Ha

**Comments on Consultative Document**
**"Sound Practices for the Management and Supervision of Operational Risk"**

Dear Madams, dear Sirs,

In its consultative document of 10 December 2010, the Basel Committee on Banking Supervision invited comments to its proposed update of the 2003 document "Sound Practices for the Management and Supervision of Operational Risk". On behalf of our five member associations representing the entire German banking sector, the Zentraler Kreditausschuss (ZKA)[1] is pleased to have this opportunity to express our views and present our position.

## General comments

The German banking sector welcomes this effort to update the 2003 document "Sound Practices for the Management and Supervision of Operational Risk" to reflect more recent developments. We would note that several of the proposed principles are, in our view, not necessarily "sound

[1] The Zentraler Kreditausschuss (ZKA) is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks financial group, and the Verband der Pfandbriefbanken (vdp), for the Pfandbrief banks.

. . .

practice" but rather, particularly for banks which apply the Basic Indicator Approach (BIA) or Standardised Approach (STA), "best practice". Some examples where we would draw this distinction are Principles 4 and 7, as well as paragraphs 25 and 40.

The consultative document proposes a number of rules which we regard as appropriate but which would not normally fall under the purview of operational risk management but rather under other risk management functions. Care must be taken that the term "operational risk" is consistent here with its definition, within the context of the first pillar, in paragraph 644 of the Basel II framework. The reference within this definition to "internal processes, people and systems" does not, in our view, provide justification to place sweeping responsibility for all risk management on the operational risk unit. There should, for example, be clarity that Principles 1 and paragraphs 21 to 23, which are board- and senior management-level responsibilities, do not, and should not be regarded as, responsibilities of the operational risk management unit. It should likewise be stated that much of Principle 9 falls within the domain of compliance or internal audit. The operational risk unit is not responsible for establishing a strong control environment but rather for identifying and controlling operational risks associated with "internal processes, people and systems". Further examples where general risk management requirements are proposed without adequately delineating the boundaries of operational risk may be found in paragraph 36 (requirement for bank staff to have necessary experience, technical capabilities and access to resources), paragraph 42 (review and approval process for new products), paragraphs 51 to 53 (creation of sound technology infrastructure) and paragraph 54 (outsourcing arrangements). Our strong view is that the existing allocation of responsibilities among organisational units is appropriate, and we would ask that this established arrangement be retained. Our concern here is that the risks named in this document will, insofar as not otherwise specified, henceforth be deemed "operational risks".

We would also mention that, within the consultative document, various proposals are made in which operational risks are linked with various permutations of the words "strategies", "products", "processes", "activities" and "systems". Our view is that this could lead to confusion or incorrect interpretations. We would thus suggest either that the phrase be used consistently or, where there is a distinction to be drawn, that this be made explicit.

We support the principle of proportionality in paragraph 5, under which the practical application of the principles of Sound Practice by an individual bank would "take account of the nature, size, complexity and risk profile of its activities". The consultative document, however, does not go on to state that these criteria may likewise be taken into account in examinations by supervisory authorities or in external audits. To avoid any misunderstandings among supervisors or external

. . .

auditors, we would suggest clarification that the proportionality principle likewise applies to their related activities.

Finally, we are concerned that a number of the rules proposed within the consultative document could impose significant additional burdens upon banks in terms of required documentation. As a general matter, documentation obligations should take into account that benefits exceed associated costs.

**Comments on particular items**

Under paragraph 11, risk management should, encompass the monitoring of risk exposures and corresponding capital needs "on an ongoing basis". We fully agree that risk exposures and capital needs must be monitored on an ongoing meaning "regular" basis, but we are concerned that this could be construed to mean "continuous". This would constitute a tightening of the first pillar requirements which we would, for practical reasons, find objectionable. We therefore kindly request that this word be changed as follows:
"*Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on a~~n ongoing~~ regular basis, taking steps to control or mitigate risk exposures…*"

In paragraph 13, as well as in paragraphs 13 and 45 of the parallel consultation document "Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches", reference is made to the "three lines of defence" for sound operational risk governance. However, the wording of the third of these is alternately called "an independent review and challenge", "independent verification and validation" and "independent review", which may cause unneeded confusion. We would therefore suggest that the third line of defence be uniformly referred to as an "independent review".

On a related point, it is our view that the option provided under paragraph 16 to have this "review and validation" (see also next point) of operational risk control mechanisms, processes and systems performed "by audit or by staff independent of the process or system under review" should not be limited to "smaller banks". Our opinion is that this alternative should be made available to all banks. The critical factor is that this review be independent of the process or system under review; the determination of who can best perform this should be left to the judgment of the individual

bank. This is particularly important within the German banking community, where it is at present broadly established practice that the internal audit unit bears responsibility for the third line of defence as described in paragraph 13. These internal audit units are strictly independent of operational risk management and, in addition, have experienced staff with the expertise to provide a professional and unbiased review.

We would specifically ask, with reference to the two preceding paragraphs, to decouple "validation" from this independent review process and thus to strike this word. The reason lies in established bank practice in Germany , which we regard to be appropriate, whereby validation is performed by the operational risk unit, then subsequently included within the scope of the independent review by internal audit. It is, in addition, unclear to us what particular elements of the operational risk framework would be validated by smaller banks, virtually all of which apply the Basic Indicator Approach (BIA) or Standardised Approach (STA).

We see no benefit in the establishment, implicit in the wording for all except smaller banks, of yet another unit independent of operational risk management. Given the overlap with established internal audit units, there would in fact be a significant duplication of efforts. Furthermore, dedicating staff to a separate unit solely for operational risk review would be, given the review cycle, an inefficient deployment of personnel.

In sum, we would ask the Committee to make the following two modifications to paragraph 16: "*…Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation and operation of the Framework. ~~For smaller banks t~~This review ~~and validation~~ may be done by audit or by staff independent of the process or system under review, but may also involve other suitably qualified parties from external sources."*

At this point, we regard the references to compensation strategies and policies in paragraph 22 as duplicative because of other recent and more specific standards which have become established supervisory practice, in particular the "FSF Principles for Sound Compensation Practices" document published by the Financial Stability Board in April 2009, along with the related Implementation Standards released in October 2009.

It is our strongly held opinion that the requirements to integrate the operational risk framework into the bank's risk management processes as outlined in paragraph 25 constitute "best practice" rather than "sound practice", and thus the present mandate should be tempered to ensure only that they are properly considered. Furthermore, the requirement to do this "across all levels of the

organisation including those at the group and business line levels, as well as into new business initiatives, products, systems and processes" is all-encompassing and would impose a significant burden in terms of documentation. We would therefore suggest, at the least, that the notion of materiality be introduced, comparable to Principle 5 ("… *Senior management is responsible for consistently implementing and maintaining* (…) *policies, processes and systems for managing operational risk in all of the bank's material products, services and activities*…").

In addition, we consider the reference here to operational risk in the context of products to be misleading. To the extent that products entail operational risks, these must be considered by the unit responsible for product development, which in turn falls under the heading of "systems".

The specific changes which we propose to paragraph 25 are thus as follows:
"*… The Framework should be appropriately integrated into the risk management processes across all levels of the organisation including those at the group and business line levels, as well as into material new business initiatives, ~~products,~~ systems and processes. In addition, results of the bank's operational risk assessment should be ~~incorporated~~ considered in~~to~~ the overall bank business strategy development processes.*"

Paragraph 27 aims to enumerate the specific policy elements which should be included in the operational risk framework. In this respect, the references in sub-paragraph (c) to permissible thresholds or tolerances for "inherent and residual risk" and in sub-paragraph (d) for their establishment and monitoring can only refer to operational risk. We would therefore ask, in the interest of clarity, to state this explicitly:

*"(c) describe the bank's accepted operational risk profile, permissible thresholds or tolerances for ~~inherent and residual~~ operational risk, and approved risk mitigation strategies and instruments;*

*(d) describe the bank's approach to establishing and monitoring thresholds or tolerances for ~~inherent and residual~~ operational risk exposure;"*

Further in paragraph 27, the term "exposure rating" used in sub-paragraph (f) is unclear to us and thus we would suggest replacing this with the unambiguous expression "risk assessment":

*"(f) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, ~~exposure rating~~ risk assessment and risk management objectives[11]"*

***Principle 3: The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.***

By calling on boards of directors not only to "oversee senior management" but, going further, to "ensure that the policies, processes and systems are implemented effectively at all decision levels", Principle 3 substantially increases board involvement in matters of operational execution. While we share the view that the board should establish the operational risk framework, its subsequent implementation once established should, in our view, be the sole responsibility of senior management. In addition, the full board should have the possibility to delegate this duty (i.e. to establish, approve and periodically review the operational risk framework) to an appropriate committee.

We regard the catalogue of board responsibilities in paragraph 28 as quite far-reaching on some points and as a clear overreach on sub-paragraph (e), which calls on the board of directors to ensure that management is actually incorporating industry best practice in managing operational risk. Here again one must draw a distinction between what is mandated "sound practice" and what is strived for, but not always immediately attainable, "best practice". We therefore request the following amendment:

*"(e) ensure that management is ~~incorporating~~ assessing industry best practice in managing operational risk."*

***Principle 4: The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.***

Principle 4 establishes a duty for the board to approve and review a "risk appetite and tolerance" statement for operational risk, implying that there is a distinction between "risk appetite" and "risk tolerance", and further calls for this to be articulated by "nature, types and levels of operational risk", which we interpret as a quantitative breakdown. Footnote 10, while drawing a fine distinction between the terms "risk appetite" and "risk tolerance" in banking practice, specifically states that the two terms are "used synonymously" in the consultative document. In order to make it clear that the board of directors of a bank, in making this statement, is not required to distinguish between these two terms, which would only serve to confuse and obfuscate the statement, we would strongly suggest (in keeping with footnote 10) to consistently use only the expression "risk tolerance", which is the appropriate term when referring to operational risks.

In addition, we regard the required breakdown by "nature, types and levels of operational risk" as a level of detail which is neither helpful nor necessary. We thus move to make the following two modifications to Principle 4:
"*The board of directors should approve and review a risk ~~appetite and~~ tolerance statement for operational risk ~~that articulates the nature, types, and levels of operational risk~~ that the bank is willing to assume.*"

Operational risks are indeed an essential component in assessing a bank's risk capacity in the context of the second pillar. We regard, however, the mandates, under paragraphs 30 and 31, for the board of directors to define "the various operational risk appetites within a bank", to establish "thresholds or limits for specific operational risks", and to review "the frequency, volume or nature of limit breaches" as inappropriate language. Operational risks, by their very nature, differ considerably from credit risks and market risks and therefore require a different approach to their characterisation. We believe that the approach of monolithically quantifying operational risks, breaking these down and setting hard limits is both misleading and impractical.

We would thus urge, in addition to the previous point raised regarding the term "risk tolerance", the following modifications to paragraphs 30 and 31:
"*30. When establishing and approving a risk ~~appetite and~~ tolerance statement, the board of directors should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. ~~The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent. The board of directors should approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.~~*

*31. The board of directors should regularly review the appropriateness of ~~limits and~~ the overall operational risk ~~appetite and~~ tolerance statement. This review should consider changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, and loss experience, ~~and the frequency, volume or nature of limit breaches~~. The board should monitor management adherence to the risk ~~appetite and~~ tolerance statement and provide for timely detection and remediation of breaches.*"

Paragraph 33 (previously paragraph 18) obligates management to "translate the operational risk management Framework established by the board of directors into specific policies and procedures that can be implemented and verified within the different business units". We are concerned that

the documentation burden which this imposes on banks could be quite extensive and would ask that this factor be taken into account in the interpretation of this statement.

With regard to the design of the operational risk governance structure, paragraph 37 (b) stipulates that the operational risk committee should, as "sound industry practice", include "independent non-executive board members", which in Germany would normally be construed as "supervisory board" (*Aufsichtsrat*). As alluded to in footnote 7 of the consultative document, the interrelationships as proposed here would be inconsistent with German law. It must therefore be made explicitly clear here that "independent non-executive board members" does not refer to supervisory board members who, for reasons of national law, may not be permitted to serve on operating bodies such as the operational risk committee. Even if there were no issue of legal separation under German law, we would consider the participation of supervisory board members in the operational risk committee to be, in most cases, of dubious benefit.

***Principle 6: Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to ensure the inherent risks and incentives are well understood.***

We agree with the premise of Principle 6 that senior management should ensure that inherent risks are properly understood by ensuring that operational risks "inherent in all material products, activities, processes and systems" are properly identified and assessed. In our view, however, the proposed additional requirement that senior management understand "incentives" relating to operational risk is neither practical nor appropriate, as this term is both vague and difficult for us to visualise in the concrete context of operational risk. We would thus move to strike this word from Principle 6 as follows:

"*Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to ensure the inherent risks ~~and incentives~~ are well understood."*

The detailed descriptions, of various instruments and methodologies for identifying and assessing operational risk in paragraph 39 are, in our view, rather unnecessary, as these terms have become broadly understood among risk professionals. We do, however, see a danger that this detailed enumeration could be easily misunderstood to mean that banks are to use some combination of these specific instruments and methodologies. The choice and design of tools for operational risk management must be left to the judgment of each individual bank based on its own circumstances.

Under paragraph 40, banks should "ensure the identification, consideration, and incorporation, as appropriate, of the operational costs and risks of operational loss in the internal pricing, performance measurement and new product approval process for all significant business lines". Given that the quantitative measurement of operational risk is a young discipline, we regard this requirement as rather ahead of its time. We therefore suggest that paragraph 40 be deferred until such time as broad agreement is reached on this complex and evolving issue.

***Principle 7: Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.***

The proposed requirement under Principle 7 for senior management to ensure an approval process for all new products, activities, processes and systems that fully assesses operational risk is, in our view, a far-reaching and significant burden, particularly for banks which apply the Basic Indicator Approach (BIA) or Standardised Approach (STA). The statement should be appropriately tempered and, to ensure that costs are commensurate with benefits, qualified in terms of materiality. We thus propose the following two modifications:

*"Senior management should ensure that there is an approval process for all new material products, activities, processes and systems that ~~fully assesses~~ considers operational risk."*

Paragraph 42 describes, in considerable detail, particular risk considerations in the review and approval process for new products, activities, processes and systems. It would seem, thus, to dictate a particular process implementation which contradicts the spirit of a document which is otherwise oriented around principles. In order to provide banks with the latitude to choose and design the most appropriate process for their individual circumstances, rather than impose one particular approach, the list of specific considerations (a) through (f) should, in our view, be stricken. We would further note here that the review and approval process of new products, activities, processes and systems does not fall within the purview of operational risk management.

We fail to understand the distinction made in the first sentence of paragraph 44, under which banks should "be able to produce reports in both normal and stressed market conditions", which implies to us a distinction in reporting. In our view, banks should be in a position to generate regular reports which apply across all kinds of market conditions. We would therefore suggest either that this distinction be deleted or that clarification be provided on how reports in stressed market conditions would differ.

According to paragraph 45 (c), operational risk reports are, among other things, to address "relevant external events and any potential impact on the bank and operational risk capital". "External events" is a rather all-encompassing concept, and because management is not omniscient, this requirement should be qualified not only in terms of relevance but also be the reasonability of presuming that management is aware of the events, which may be relevant but far away or not widely publicised. We would thus propose that the following phrase be appended:

*"(c) available relevant external events and any potential impact on the bank and operational risk capital."*

Paragraph 52 mandates an "integrated approach to identifying, measuring, monitoring and managing" risks associated with technology. While we fundamentally regard this requirement as sensible and appropriate, it is, in our view, already explicit, under paragraph 644 of the Basel II framework, that operational risk specifically includes "systems" and thus would seem to us superfluous. Principle 7 likewise requires an operational risk-based approval process for all new products, activities, processes and systems. In order to eliminate unnecessary redundancy, we suggest that paragraph 52 be stricken in its entirety.

Paragraph 55 includes, in the context of risk insurance or other risk transfers, the requirement for the board to perform an "annual review of the bank's risk and insurance management programme". For banks with simple business models, we regard this requirement as rather rigid. So that there is a degree of latitude, under the proportionality principle, to consider the individual circumstances of the bank and the relevance of these risk insurance arrangements, we would suggest that the appropriate time period for review be left to the judgment of the bank, as follows:

"*…The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform ~~an annual~~ reviews of the bank's risk and insurance management programme after appropriate periods of time.*"

Under paragraph 58, banks are to develop business continuity plans, commensurate with the nature, size and complexity of their operations, which analyse the impact of plausible disruptive scenarios and define appropriate contingency strategies and recovery measures. It goes on to stipulate "communication plans for informing management, employees, regulatory authorities, customer[s], suppliers, and – where appropriate – civil authorities". We regard the implied mandatory inclusion of customers and suppliers in all contingency communication situations as excessive. Rather than imposing a general requirement to necessarily inform suppliers and customers, banks should have the latitude to determine, in their best judgment, when it is necessary

and appropriate to provide this kind of information to the external market. We would thus request that the specific (and implicitly mandatory) inclusion of customers and suppliers be removed as follows:

"*Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, ~~customer[s], suppliers,~~ and – where appropriate – civil authorities."*

If we can be of any further assistance, or if you have any questions, please feel free to contact us.

Yours sincerely,
on behalf of the Zentraler Kreditausschuss
Association of German Banks

Dirk Jäger

Anja Schulz