Enhancements to Basel II "Principles for the Sound Management of Operational Risk" and required revisions to the CBB Rulebook

Industry Comments and Feedback
Volume 2
September 2012

Industry Comments		
General Comments:	**Ref**	**CBB's Response**
A bank suggested the following: 1. The operational risk framework should give due consideration to smaller institutions which may not need or be able to have dedicated staff/ resources for each area, such as Internal Audit or Compliance.	GR1	Noted.
2. The framework proposed in the Consultation Paper appears to be more applicable to the commercial banks. The CBB should perhaps include a separate framework, appropriately modified, related to the wholesale banks.	GR2	Disagree- Basel requirements apply to all banks. An operational fault in a wholesale bank may have just as catastrophic or material effect as a fault in a commercial bank..
A bank noted that there appears to be a minor discrepancy between the consultative paper and its equivalent Basel document in that the BIS documents at paragraph No.14, No.15 and No.16 talks about three lines of defenses for management of operational risk. Whereas, paragraph No. OM-8.1.5 of the consultative paper does not address the first line of defense which is the business line management.	GR3	**Disagree-**OM-8.1.4 "a Guidance Paragraph" presents the three lines of defense of the sound operational risk governance similar to those presented in the Basel paper. Which are: (a)Business line management; (b)An independent operational risk manageme function; and (c)Independent review functions.

Further, will the CBB give banks sufficient time to comply with the revised rules once enacted?	GR4	Banks will be required to prepare a gap analysis in order to identify their compliance plan and the time required for implementation.
A bank noted the following: • There is strong reason to believe that the exposure to operational risks in the future will increase. The reason is that technology changes escalates threats, financial products become increasingly complex and interconnected, especially if financial institutions decide to outsource vital parts of their services, unpredictable politics climates, and an increase blurring of the effect of cross-boarders regulations (e.g. Foreign Account Tax Compliance Act - FATCA). Therefore, it is important to maintain a balanced approach for the use of qualitative assessments and quantitative assessments across current risks, forecasted risks, and realized risks.	GR5	Noted.
• When it comes to qualitative risk to be mapped to money, beside it is a challenging task, there will always be a tension between the top-down imposition of a charge by the central bank and the bottom-up nature of detailed decisions which is required to be made by financial institutions. One of the challenges is the potential for misrepresentation. It is recommended that ICAAP and the quality of risk management together to form a view on the appropriateness of the bank's internal capital targets and its capacity for meeting the targets.	GR6	Noted.
• Insurance Policy plays an important role in decreasing the financial impact of operational losses and can therefore contribute to a better performance by covering a variety of potential operational losses. So, will CBB allow banks to get use of insurance to optimize the capital required for operational risk for	GR7	Basel does not recognize insurance as a mitigant for capital adequacy purposes.

banks, i.e. to consider the risk mitigating impact of insurance in the measuring of operational risk used for regulatory minimum capital requirements? And if yes, what would be the recognition limit as % of the total operational risk capital charge. It is important to bear in mind that some issues will remain hurdle, such as: • Unlike market or credit risk, it is difficult to determine whether the portfolio of operational risk for a bank is complete • Operational risk has been described as the oldest of risks; yet operational risk management is one of the newest of disciplines. Following the current crises, the weight of operational risk has risen to the point that operational risk is not just another type of risk but holds a significant position in risk assessment. However, the difficulty in validating operational risks in all models reduces the reliability or usefulness of these models in predicting future outcomes.	GR8	Noted.

Specific Comments:			
Reference to the draft Directive:	**Comments**	**REF**	**CBB's Response**
OM-8.1.5 **The operational risk management function must be functionally independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk Framework ("Framework") within the bank.**	**A bank** noted that the word Framework is not defined in the Glossary of the CBB Rulebook, therefore it will be useful to include the CBB's precise definition for the word Framework (i.e. Operational Risk Framework).	SP1	Noted, a definition will be available in the Glossary of the Rulebook
	In addition, this rule is only separating between Risk Management Function and Business Lines who generate risks, however other functions do generate risks, therefore, it will add clarity to state that the risk management function must be functionally independent of risk generating business lines / support function etc.	SP2	The rule states that operational risk management function must be functionally independent of any/all risk generating business lines, which includes other functions.
OM-8.1.6 The operational risk management function should include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the operational risk management function is to challenge the business lines' inputs to, and outputs from, the bank's risk	**A bank** noted that due to the importance of this guidance and the high level requirements it addresses, it is suggested that this paragraph should be reflected as a Rule rather than Guidance.	SP3	**Disagree-** this paragraph is to remain as a guidance.

management, risk measurement and reporting systems. The operational risk management function should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.			
OM-8.2.6 **Compensation policies must be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They must also appropriately balance risk and reward.**	**A bank** noted that compensation policies must be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They must also appropriately balance risk and reward. A cross reference might be useful to Chapter **HC-5.**	SP4	The CBB has drafted a separate consultation on Basel principles issue on compensation and it is now under internal discussion.
OM-8.2.8 **Principle 2: Banks must develop, implement and maintain a <u>Framework</u> that is fully integrated into the bank's overall risk management processes. The <u>Framework</u> for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.**	**A bank** noted that the operational risk management framework is to be dependent "on a range of factors, including its nature, size, complexity and risk profile". The bank appreciates the option to customize an operational risk management framework given the Bank's business model which dictates lower number of client relationships and volume of transactions vs. institutions having multi-location or retail operations.	SP5	It is the responsibility of the Board to establish a "Framework" that suits the nature of the bank.

OM-8.2.17 **When approving and reviewing the risk appetite and tolerance statement, the board of directors must 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 must approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance.**	**A bank** suggests to add the word "operational" as follows: **"**when approving and reviewing the **Operational** risk appetite and tolerance statement, the board of directors must 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 must approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite and tolerance". Since that this chapter is particularly about Operational Risk, adding the word Operational will add clarity.	SP6 SP7	Noted.. Basel appears to be noting that there is a general risk statement to be made and operational risk is an important component of this statement. Adding the word 'operational' will also limit it to operational risk, which does not appear to be the intention of the Basel Committee..
OM-8.2.20 **Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These must include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks must be able to demonstrate that the three lines of defence**	**A bank** suggested adding a reference as follows: "Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These must include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks must be able to demonstrate that the three lines of defense (as highlighted in **OM-8.1.4**) approach is	SP8	Noted.Cross reference added.

approach is operating satisfactorily and to explain how the board and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner.	operating satisfactorily and to explain how the board and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner". A cross reference might be useful to paragraph **OM-8.1.4.**		
	One observation is noted here. Paragraph **OM-8.2.20** is a Rule that is obliging the Banks to make sure that the three lines of defense (as highlighted in paragraph **OM-8.1.4**) are operating satisfactorily. However the three lines of defense are introduced as guidance since that paragraph **OM-8.1.4** is considered as guidance. To be consistent, either paragraph **OM-8.1.4** should be upgraded to a Rule or paragraph **OM-8.2.20** becomes guidance.	SP9	**Disagree**- OM-8.2.20 is a mandatory "Rule" and for further details on the implementation, banks can refer to"Guidance".
OM-8.2.22 **Senior management must ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance**	**A bank** noted that given the business nature and size, the Bank does not employ a tripod structure of risk management i.e. individual people or section responsible for three main risks i.e. credit risk, market risk and operational risk. Beside the Board Risk Committee, risk exposures are managed at various Management levels. At operating level, concerned risks exposures are "owned" and managed by respective	SP10	The paragraph does not require a tripod structure of risk management. It simply requires effective communications. OM-8.2.30 is a "Guidance" which covers the point raised by VC Bank in its suggestion.: "*Risk identification and assessment are fundamental characteristics of an effective operational risk management system.*

risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.	departments and the Executive Management Committee. Independently, the Risk Management Team identifies, assesses, reports and recommends any necessary mitigation measures – whose efforts are subject to Internal Audit's periodic review. Hence, it may be impractical to have such segregation of duty within the risk management function for each risk area. Adding the below paragraph might add additional clarity in this regard: The bank's Risk Management Function should be commensurate with the nature, size, complexity and risk profile of its activities.		*Effective risk identification considers both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover) and external factors (such as changes in the broader environment and the industry and advances in technology). Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively*".
OM-8.2.53 The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass: (a) Procedures for determining	**A bank** noted that Chapter OM-3 (Outsourcing) is detailed and comprehensive i.e. it will be more consistent to remove paragraph **OM-8.2.53** from section OM-8.2 and included under Chapter OM-3 as a guidance.	SP11	**Agree-** to re-locate OM-8.2.53 & OM-8.2.56 to chapter OM-3 (Outsourcing) & chapter OM-5 (Business Continuity Planning) respectively to avoid redundancy.

whether and how activities can be outsourced; (b) Processes for conducting due diligence in the selection of potential service providers; (c) Sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights; (d) Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider; (e) Establishment of an effective control environment at the bank and the service provider; (f) Development of viable contingency plans; and (g) Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.			

OM-8.2.56 **Principle 10: Banks must have business resiliency and contingency plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption. Business continuity is discussed in more detail in Chapter OM-5.**	**A bank** noted that Chapter OM-5 Business Continuity Planning is very detailed and comprehensive, the cross reference provided in Paragraph **OM-8.2.56** is sufficient. (i.e. paragraph OM-8.2.58, OM-8.2.59, OM-8.2.60 are repetitive of the content and spirit of chapter OM-5).	SP12	**Agree-** to re-locate OM-8.2.53 & OM-8.2.56 to chapter OM-3 (Outsourcing) & chapter OM-5 (Business Continuity Planning) respectively to avoid redundancy.
OM-8.3.4 **A bank using the standardised approach must meet the following additional criteria:** **(a) The bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function. The operational risk management function is responsible for developing strategies to identify, assess, monitor and control/mitigate operational risk; for codifying bank-level policies and procedures concerning operational risk management and controls; for the design and implementation of the bank's operational risk assessment methodology; and for the design**	**A bank** noted that in the two high level sub paragraphs (d) and (e) are applicable for both approach i.e. they should **not** be viewed as an additional criteria only for the standardized approach.	SP13	**Agree-**. Items (d) and (e) are already listed as part of the basic Indicator Approcah, therefore, should be deleted from this OM-8.3.4.

and implementation of a risk-reporting system for operational risk; **(b) As part of the bank's internal operational risk assessment system, the bank must systematically track relevant operational risk data including material losses by business line. Its operational risk assessment system must be closely integrated into the risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the banks operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, and risk analysis. The bank must have techniques for creating incentives to improve the management of operational risk throughout the bank;** **(c) There must be regular reporting of operational risk exposures, including material operational losses, to business unit management, senior management, and to the board of directors. The bank must have procedures for**			

taking appropriate action according to the information within the management reports; **(d) The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of noncompliance issues;** **(e) The bank's operational risk management processes and assessment system must be subject to validation and regular independent review. These reviews must include both the activities of the business units and of the operational risk management function; and** **(f) The bank's operational risk assessment system (including the internal validation processes) must be subject to regular review by external auditors and /or the CBB.**			