From:	Brian Barnier
To:	Basel Committee, Service
Subject:	FW: Organization Comment on Sound Practices Consultative Paper
Date:	Thursday 30, December, 2010 03:59:28
Attachments:	Brian Barnier.vcf Comments_on_the_Sound_Practices_Consultative_Paper As Submitted.doc

Greetings Members of the Committee,
Attached are comments on the Sound Practices for the Management and Supervision of Operational Risk.
While these are submitted only in the context of ValueBridge Advisors, the authors (Gabriel David and Brian Barnier) serve in a variety of capacities with several professional associations and business organizations, and have been globally recognized for their contributions to industry standards and practices, teaching, government service and research in the field of risk management. Bios are available on request.
Should you have any questions, please do not hesitate to contact us.

Best Regards,

Brian Barnier and Gabriel David

Brian Barnier
Envision - Align - Focus - Execute
ValueBridge Advisors
brian@valuebridgeadvisors.com
+1.203.295.0426 x703
AOL IM and Yahoo IM screen name BrianBarnier
News of "green shoots" and risk on www.twitter.com\Brian_Barnier
Team blog & videos: risktech.financetech.com

Comments on Sound Practices for the Management and Supervision of Operational Risk

13. “Three lines of defence” is helpful. However, it is an assurance concept, rather than performance management and daily use of risk in the management of operations. Assurance approaches (periodic in nature) have a tendency to divert focus from performance-oriented risk management in daily business. It also confuses the role of risk management between managerial and assurance. From a terminology point of view, it stresses just three items in the chain that might include business line management, performance management (finance, process improvement, quality, more), risk management, internal control, internal audit (including outsourced audit functions), external audit and examinations. Suggest either deleting or placing clearly in the context of assurance (and, if assurance, extending with other lines).

15. The notion of the CORF is useful. As above, suggest defining clearly between a managerial and assurance role. Institutions that are unclear on this seem to waste resources that could otherwise be used to daily reduce risk to operations.

Principle 2. Suggest providing more guidance on elements of a “Framework.” The superficial frameworks often used in operational risk in financial institutions (in contrast to those in other industries and disciplines) seem to be a significant cause of weak risk management capability development and the resulting outcomes. Recognized industry “frameworks” for management processes typically include

- What to do: Process Model Steps
    - Management practices
    - Input – Output Tables
- What to measure: Goals and Metrics tables
- Who does it: Responsible, Accountable, Consulted, Informed (RACI) Tables
- How to Measure and Progress: Maturity Models or Agreed Upon Procedures
- Glossary/Consistent Terminology

These framework elements are especially needed to see interdependencies between types of risk (operational, market and credit with liquidity and reputation impacts) and systemic issues. For example, using such a framework provides specifics on how to mitigate risk in each area process steps, goals and metrics, RACIs, evaluate and terminology. Recommend either here or in paragraph 27 explicitly stating the framework elements mentioned above.

Footnote 10: Suggest increased caution on using “appetite” and “tolerance” synonymously because the a) confusion of these terms in practice and b) document continues to use both terms individually. Suggest referring to them in plain English, rather than term of art.

Principle 9: This principle suggests that the majority of risks are responded to with controls. In practice, a range of other responses are needed (especially for environmental and process capability related risk).

The sentence shows this difficulty by defining "control" as one element of the definition of "control" used in the first clause. Would suggest titling this principle "Risk Response," include a broader lists of potential response actions and simplify the second clause. Thus, would read "Banks should have a strong risk response approach that utilises: monitoring, early warning, preparation, policies, processes, systems, controls, and other risk mitigation and/or transfer approaches."

Principle 10: "Resiliency" is a term that doesn't seem to translate into many other languages. A survey a few years ago reported lack of clarity. Even in English, there is little industry clarity on the difference between "resilience" and "continuity." If there is a distinction intended, then suggest specifying it. If there is no distinction intended, then suggest using only one term to avoid confusion.

Paragraph 23: As part of determining training needs, suggest adding as one of the criteria "identified weaknesses in risk management capability." This could be refined to include specifics in areas such as dependency, scenario, systems, product and process analysis that are often overlooked in departments that staff with compliance-oriented (instead of management) skills.

Paragraph 25: It is commendable to integrate ops risk into risk management and business strategy. Suggest also integrating into all governance structures and operations management – this is the direct connection to embedding risk in the daily business use. In addition, suggest connecting into paragraph 42 and the product management process, especially for fraud prevention.

Paragraph 27©: Suggest caution in using the term "residual risk." This term can be misleading providing a false sense of confidence when risks are a) only partially "controlled" when other measures are appropriate and b) the residual risk changes far more frequently than evaluations or current monitoring. "Inherent risk" is also less than precise. To achieve the Committee's objective and overcome confusion, suggest revising to "permissible thresholds or tolerances for risk on appropriate time intervals (minute, day, month, year)."

Paragraph 28: To the list of items for the board of directors, would add:

- "Regularly review status on a) improved operational performance outcomes as a result of operational risk management actions, b) efficiency and effectiveness of operational risk management function, and c) improvements in operational risk management capabilities (skills, tools, resources)"
- "Regularly review metrics associated with root cause status and post incident reviews to understand a) how well causes are understood, b) likelihood of problems occurring and b) status of actions to address root causes monitored in daily operations or identified in incident reviews."

This would surface to board level points made by the Committee elsewhere in the document (such as in product or process management) and equips the board with specific information that enables them to more fully appreciate the specifics of the risk taken and exercise meaningful oversight.

Paragraph 29: “The phrase operational risk control” is used here whereas otherwise (with only one exception) “operational risk management” is used throughout. The phrase “risk control” often contributes to two types of confusion: 1) between the managerial and assurance roles, and 2) a fallacy that controls are sufficient to manage risk. Suggest replacing with “operational risk management.”

Paragraph 39b: Suggest noting that losses would include all losses incurred in an unfolding chain of events, rather than the loss at any given point in the chain. This is also key to the Committee’s objective of making interdependencies in systems more visible.

Paragraph 39c: RSCA’s are helpful in their proper role. However, they also have weaknesses. These include: Failing to verify prerequisites. Failing to recognize the rate of change. Failing to understanding core process weaknesses. Failing to embed risk management into the business. Failing to focus, diverting resources. The positioning of RSCA in this paragraph seems to put an overreliance on the technique, making it the only approach to achieve the objectives of the paragraph title “Risk Assessment.” In broader industry and discipline use, RSCAs are one of many techniques, less effective than most and not widely used outside of evaluating controls to financial reporting. Suggest focusing on “risk assessment” throughout and either eliminating the reference to RSCAs or including it in a list of techniques (led by more robust scenario analysis (please see comments below). An example of such a list is in the appendix to A Risk Management Standards (ARMS) published by The IRM, ALARM and AIRMIC in the U.K. We can provide others.

Paragraph 39d: Commendable addition on business process analysis.

Paragraph 39e: Suggest more direct wording. KPIs and KRIs are directly paired. A KRI measures the risk that the KPI will not be achieved. KRIs can be applied at several levels (this has contributed to the loose usage of the term KRI). These levels include key drivers and then broader root causes (as it is difficult to know which root cause will drive the loss). This not only clarifies, but also pragmatically is an effective way to more deeply integrate risk into business reporting and decision-making.

Paragraph 39f: “Scenario analysis” is defined softly and broadly. We recommend more precisely defining that scenario analysis is designed to bring together the information from the environment and capabilities to tell a story about the risks to the institution, gain insight on dependencies, and understand the ability to detect unfolding events, likelihood and impacts. This includes interdependencies between market, liquidity, credit and operational risks that occur in the real world. While it does use qualitative information, the word “opinion” suggests a laxness in application that is inappropriate. To avoid bias, the analysis should be structured to understand how the operations work within an environment. Bringing the “robust scenario analysis” language of the Supervisory Guidance for the AMA Approaches consultative document into this document would be helpful. However, even that document accepts a more soft view of scenario analysis than is generally used outside of financial institution operational risk departments. It would be helpful to draw in the rigorous body of knowledge around the analytical use of scenarios used elsewhere in financial institutions and other industries.

Paragraph 42: Commendable addition on new product management – it should be explicit that this also extends to all areas of financial services. Minor suggestion to emphasize using product analysis especially to prevent fraud. Suggest also stating "product management cycle" rather than "new product" to more deeply embed risk-awareness in the product management lifecycle and tap into the risk management considerations that already exists in the product management discipline.

Paragraph 45: Suggest explicitly reporting on operational risk management capability (skills, processes governance, measurement and tools). This would provide a feedback mechanism to points mentioned earlier.

Paragraph 48-50: The terms control, policy and procedure are used almost interchangeably and without distinction. Clarity is necessary to avoid confusion. The bullets listed are primarily policies, rather than controls.

Paragraph 51-59: We recommend using ISACA's Risk IT Based on COBIT and Control Objectives for Basel II for considerations on strengthening these paragraphs and reconciling them to widely used international guidance. This would make it easier for institutions to implement these paragraphs. This guidance is already recommended or required in a number of countries. In addition, specific guidance is necessary on the outsourcing topic – more details are required and offshoring should be specifically addressed as an IT-related business risk. In addition to ISACA's COBIT, The Shared Assessment Program provides helpful guidance that is mapped to COBIT, U.S. FFIEC and other guidance.

Paragraph 58. This creates a new notion of a "resilience level" that might add to terminology confusion that already exists. We recommend a description in plain English. "Scenarios" used here could be tied back to 39f to provide consistency. Also, as scenarios used for business continuity/disaster recovery/crisis management today tend to be more robust than the limited scenarios often used for long tail testing, this provides the opportunity to connect those thoughts within the document to bring scenario experience from BC/DR/CM into broader operational risk use.

Paragraph 57-59. Feels a bit like an add-on to the rest of the document. You might wish to integrate more into overall management of risks to operations. In doing so, it could also reference other areas of risk management (e.g., project, security, facilities, outsourcing, change management, energy) that relate to operations.

Paragraph 61. Suggest adding "capabilities" to "framework" as capabilities are both a key driver of framework quality and most proximate to improved risk management outcomes.

Respectfully Submitted,
Brian Barnier, brian@valuebridgeadvisors.com
Gabriel David, gabedavid@gmail.com
ValueBridge Advisors