KPMG
cutting through complexity™

Regulatory Practice Letter
November 2014 – RPL 14-18

BCBS Issues Bank Progress Report on Principles for Sound Operational Risk Management

Executive Summary

The Basel Committee on Banking Supervision ("BCBS" or "Basel Committee") issued a report on October 6, 2014, entitled *Review of the Principles for the Sound Management of Operational Risk*. The report serves as a review of systemically important banks' ("SIBs" or "banks") implementation of the Basel Committee's *Principles for the Sound Management of Operational Risk* ("Principles"), which were published in June 2011 and cover governance, the risk management environment, the role of disclosure, and the three lines of defense.

The review, conducted in the form of a questionnaire for banks to self-assess their implementation progress, surveyed sixty SIBs operating in twenty jurisdictions. The objectives of the exercise were to establish the extent to which banks have implemented the Principles, identify common significant implementation gaps, and highlight emerging and noteworthy operational risk management ("ORM") practices that are not currently addressed by the Principles.

Although the review identified challenges and themes within all of the Principles, four Principles were identified among the least thoroughly implemented, including: (1) operational risk identification and assessment, (2) change management, (3) operational risk appetite and tolerance, and (4) operational risk disclosure. In addition, weaknesses were observed in banks' implementation of the overarching Principle for the three lines of defense.

The report concludes that, based on the responses received, SIBs have generally made "insufficient" progress in implementing the Principles, with many banks still in the process of implementing various ones. As a result, some SIBs may not be adequately identifying and managing their operational risk exposures due to the inconsistent deployment of the full range of ORM tools, such as risk and control self-assessments ("RCSAs"), internal and external loss data collection and analysis, scenario analysis, key risk indicators ("KRIs"), key performance indicators ("KPIs"), change management, and comparative analysis. Additionally, banks will need to strengthen their implementation of the "three lines of defense" Principle, including clarifying roles and responsibilities, as well as improve their board and senior management oversight, their articulation of their operational risk appetite and tolerance statements, and the comprehensiveness of their operational risk disclosures.

Background

The financial crisis revealed the need for banks to fully implement appropriate operational risk identification and management practices in order to mitigate direct and material financial losses, reputational and consequential risk, and systemic shocks to other banks, customers, counterparties, and the broader financial system. To address these concerns, the BCBS published an update to its February 2003 guidance entitled *Sound Practices for the Management and Supervision of Operational Risk* in June 2011, which detailed eleven fundamental Principles for governance, the risk management environment, and the role of disclosure, as well as one overarching Principle for the three lines of defense. According to the Basel Committee, the updated paper enhances the 2003 sound practices guidance by including the following specific ORM Principles considered to be consistent with sound industry practices:

- *Operational risk culture (Principle 1):* A bank's board of directors and senior management should establish a strong risk management culture throughout the entire organization that supports and provides appropriate standards and incentives for professional and responsible behavior.
- *Operational risk management framework (Principle 2):* A bank should develop, implement, and maintain a framework that is fully integrated into its overall risk management processes, commensurate with its nature, size, complexity, and risk profile.
- *Board of directors (Principle 3):* The board of directors should establish, approve, and periodically review the ORM framework and oversee senior management to ensure that the policies, processes, and systems are implemented effectively at all decision levels.
- *Operational risk appetite and tolerance (Principle 4):* The board of directors should approve and review a risk appetite and tolerance statement that articulates the nature, types, and levels of operational risk that the bank is willing to assume.
- *Senior management (Principle 5):* Senior management should develop a clear, effective, and robust governance structure for board approval that demonstrates well defined, transparent, and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining ORM policies, processes, and systems in all of the bank's material products, activities, processes, and systems consistent with its risk appetite and tolerance.
- *Operational risk identification and assessment (Principle 6):* Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes, and systems to make sure the inherent risks and incentives are well understood.
- *Change management (Principle 7):* Senior management should ensure that there is an approval process that fully assesses operational risk for all new products, activities, processes, and systems.
- *Monitoring and reporting (Principle 8):* Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses, and establish appropriate reporting mechanisms that support proactive ORM at the board, senior management, and business line levels.
- *Control and mitigation (Principle 9):* A bank should have a strong control environment that utilizes policies, processes and systems, appropriate internal controls, and appropriate risk mitigation and/or transfer strategies.
- *Business resilience and continuity (Principle 10):* A bank should have business resiliency and continuity plans in place to ensure its ability to operate on an ongoing basis and limit losses in the event of a severe business disruption.

- *Role of disclosure (Principle 11):* A bank's public disclosures should allow stakeholders to assess its approach to ORM.
- *Overarching Principle of the three lines of defense:* A bank has established the roles and responsibilities of the three lines of defense, defined as business line management, an independent corporate ORM function ("CORF"), and an independent review.

The BCBS noted that these Principles establish sound practices relevant to all banks. Banks should take into account the nature, size, complexity, and risk profile of their activities when implementing these Principles.

Description

In early 2014, the BCBS conducted a review of sixty SIBs with operations in twenty jurisdictions[1] on their implementation of the Principles that included a specific focus on assessing the three lines of defense. Designed as a questionnaire for participating banks to self-assess their implementation progress, the review was conducted under the overall supervision of the Basel Committee and the banks' respective supervisory authorities. However, the BCBS noted that the review did not involve an onsite validation of the banks' responses to the 180 questions posed in the review.

Key Findings from the SIBs' Self-Assessments

Although the review identified areas of improvement within each of the Principles, the BCBS highlighted the following Principles among the least thoroughly implemented:

Operational Risk Identification and Assessment (Principle 6)

The review found that, while banks have implemented some of the operational risk identification and assessment tools, other tools have either not been fully implemented or have not been used effectively for risk management purposes. Some banks reported that the tools they have implemented were largely used for risk measurement purposes (e.g., capital measurement and allocation), while others indicated that they have not fully implemented the tools because they were deemed unnecessary for risk measurement purposes.

In addition, the review found that banks reported a wide range of practices regarding their implementation of many of the tools. For instance, while many banks have implemented distinct, multi-tiered tools, such as RCSAs, scenario analysis, and business process mapping, some banks noted that they have chosen to implement one tool to serve the purpose of two or possibly three tools, such as a scenario- or process-based RCSAs. The report concludes that, for some banks, considerable management effort will be required to ensure bank-wide implementation of certain tools, including improving: (1) KRIs/KPIs, (2) external data collection and analysis, (3) comparative analysis, and (4) the creation and monitoring of action plans generated through the use of the tools.

Change Management (Principle 7)

The BCBS observed that the change management Principle had one of the lower average ratings assigned, indicating that banks are continuing to implement and

[1] Participating jurisdictions for the bank questionnaire included Australia, Belgium, Brazil, Canada, China, France, Germany, India, Italy, Japan, Netherlands, Russia, Saudi Arabia, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, and the United States.

enhance their existing change management programs, such as new products and initiatives. Approximately two-thirds of the banks reported having fully implemented RCSAs within their change management process for new products and initiatives. Similar to the implementation of the operational risk identification and assessment tools, the report identified a wide range of practice related to the policy framework for change management processes. For example, a few banks reported that their governance framework did not apply to all types of change, such as outsourcing oversight. Many banks also noted that the operational risk taxonomy is either applied inconsistently or not applied at all to various changes including new products, activities, processes, and systems. Consistent alignment with the bank's taxonomy would allow for the integration and aggregation of results with its overall risk profile.

Several banks noted that the roles and responsibilities relating to change management were included within either the bank's ORM framework or underlying change management-related policies. Many banks also noted the involvement of several control groups within the second line of defense review of RCSAs, such as compliance, legal, business continuity, technology, and other risk management groups. However, a number of banks continued to state they had not yet fully implemented the second line of defense responsibilities related to change management.

In addition, a small number of banks noted that these other control groups were primarily responsible for performing the RCSAs, which the Basel Committee did not consider to be fully aligned with the concept of the three lines of defense. Some banks also noted that the CORF was only involved in the process through membership in an approval and oversight committee. The BCBS also stated that participation in a committee may not fully allow for the opportunity to provide an effective challenge to the first line of defense's RCSA program.

Lastly, many banks reported either an absent or partially implemented process for monitoring risks following the approval of an initiative, as well as an absence of a formal post-implementation review process.

Operational Risk Appetite and Tolerance (Principle 4)

Many banks generally indicated that establishing a risk appetite and tolerance statement was more challenging for operational risk than for other risk categories, such as credit and market risk. Although this difficulty was attributed to the nature and pervasiveness of operational risk, for the banks that have established a statement, the inclusion of a metric, such as operational losses as a percentage of gross revenue, was a commonly observed practice. However, because these metrics tend to be backward- rather than forward-looking, many banks indicated that they are currently working to enhance their existing statements.

Role of Disclosure (Principle 11)

Most banks reported that, in general, the quality of operational risk disclosure is fully compliant, pointing to either a specific section for operational risk in their annual reports or individually developed templates under the existing Basel Framework's Pillar 3 disclosure requirements. However, the BCBS pointed out that these disclosures do not contain sensitive information relating to control gaps or issues, which suggests that they tend to be primarily high-level statements. The Basel Committee surmised that the relative lack of information on the banks' operational risk

profile and ORM processes may be attributable to inadequate implementation of a disclosure policy that is subject to approval and oversight by the banks' board.

Overarching Principle of the Three Lines of Defense

Although most banks reported that they comply fully with the three lines of defense Principle, the BCBS also found a range of existing practices related to its implementation. In a few cases, SIBs inappropriately classified responsibilities across each of the three lines of defense, such as assigning various business line responsibilities to the second line. Many banks noted that they are still in the process of implementing a more refined approach to the assignment of specific responsibilities to the three lines of defense.

Some banks also reported more significant challenges related to both inconsistent application and their ability to substantiate the independent review of the ORM tools used by the first line, while a few banks specifically noted insufficient resources within the CORF. In addition, a large number of banks have yet to fully develop a quality assurance ("QA") program within the second line that ensures the consistent application of an independent challenge.

Most banks indicated that third line responsibilities were fulfilled, noting that entities performing the review and challenge of the design and effectiveness of the bank's ORM controls, processes, and systems are not involved in the development, implementation, and operation of the ORM framework, and that internal audit coverage of the framework is adequate. Although most banks indicated that internal audit has sufficient resources to carry out its third line responsibilities, a few banks noted that their third line responsibilities needed improvement in terms of definition, execution, and monitoring, and that staffing within internal audit was insufficient.

The review of both the first and second lines was reported to be sufficient and commensurate with other risk management functions that follow a risk-based approach when determining the frequency and scope of an audit. However, almost a third of the banks reported that further enhancements were needed or planned to ensure full compliance, with some banks noting that coverage was limited to the operational risk model and its inputs, rather than the implementation of the overall ORM framework.

Commentary

The BCBS peer review observations provide important benchmarking insights regarding the evolution of ORM practices and the continued challenges large financial institutions face in addressing heightened regulatory expectations. The BCBS observations are consistent with the findings revealed in the *KPMG/RMA Operational Risk Management Excellence – Get to Strong Survey*, which also showed that participating financial institutions are at various stages of implementing their ORM programs, and the analysis provided in KPMG's *The Changing Face of Regulatory Reporting: Challenges and Opportunities for Financial Institutions Point of View*. In addition, the Principles complement the Office of the Comptroller of the Currency's ("OCC's") final *Heightened Standards* guidelines[2] and the BCBS's *Principles for*

[2] See *KPMG Regulatory Practice Letter 14-14*.

Effective Risk Data Aggregation and Risk Reporting,[3] as well as certain final provisions of the *Section 165* rulemaking[4] under the *Dodd-Frank Wall Street Reform and Consumer Protection Act*.

As such, large banks should expect heightened supervisory focus on the application of sound ORM Principles within their firms. Specifically, the findings in the BCBS report reinforce the need for banks to continue their efforts to proactively address the following areas when enacting their ORM programs:

- Improve **risk identification and assessment**, including:
  - Developing and implementing tools, such as RCSAs, KRIs/KPIs, external loss data, business process mapping, comparative analysis, and operational risk scenarios for enterprise-wide risk management assessment purposes; and
  - Creating, monitoring, and remediating action plans generated from all tools.
- Strengthen implementation of the **three lines of defense** model, including:
  - Refining and enhancing the assignment of roles and responsibilities to relevant departments;
  - Involving corporate control groups with relevant expertise (e.g., compliance, legal, business resilience and continuity, technology, and other risk management groups) in supporting the second line;
  - Ensuring that an independent challenge is consistently applied by implementing a QA program within the second line; and
  - Ensuring that there is sufficient focus and coverage within the audit plan on the ORM framework.
- Enhance the **ORM framework**, including:
  - Integrating the ORM program into the strategic decision-making process; and
  - Requiring a robust operational risk assessment process within the new product and initiative approval process.
- Enhance the comprehensiveness, implementation, and monitoring of **change management** programs and processes, including ensuring that the roles and responsibilities are aligned with the three lines of defense Principle.
- Reinforce **ORM culture** through training and awareness programs, an active communication strategy, and alignment of compensation policies with operational risk appetite.
- Improve **monitoring and reporting**, including:
  - Requiring the use of an operational risk taxonomy in all ORM tools to allow for the aggregation and reporting of risk and control issues;
  - Developing and testing the effectiveness of data-gathering and aggregation in a stressed condition;
  - Developing a flexible process for extracting data on-demand; and
  - Improving the quality and timeliness of external loss events.
- Improve **board oversight** of bank managements' recommendations and decision making, including documenting instances of appropriate credible challenge.
- Articulate and implement enhanced and forward-looking **operational risk appetite and tolerance** statements.
- Improve ORM public **disclosure**, including:
  - Developing a comprehensive policy for board approval and oversight that is subject to independent review; and
  - Enhancing disclosure on the management of operational risk exposures.

[3] See *KPMG Regulatory Practice Letter 14-01*.
[4] See *KPMG Regulatory Practice Letter 14-07*.

Notably, the BCBS report encourages banks to consider more formal processes for benchmarking external ORM practices, including periodically engaging "independent external advisors" to assist them in analyzing banks' ORM frameworks as a part of their regulator assessment of its design and effectiveness.

Lastly, banks will likely need to demonstrate to supervisors that their implementation of the Principles is fully aligned with their risk profile and that their methods for identifying and managing operational risk are complementary to, as opposed to a consequence of, the more quantitative methods employed for calculating their operational risk capital requirements.

This is a publication of KPMG's Financial Services Regulatory Risk Advisory Practice and the Americas' Financial Services Regulatory Center of Excellence

For additional information, please contact:
Hugh Kelly, Principal: hckelly@kpmg.com
David Stone, Director: dstone2@kpmg.com

Author: Lisa Newport, Assoc. Director, Americas' Financial Services Regulatory Center of Excellence: lisanewport@kpmg.com

Earlier editions are available at:
www.kpmg.com/us/regulatorypracticeletters