KPMG
cutting through complexity™

Regulatory Practice Letter
January 2014 – RPL 14-01

BCBS Issues Bank Progress Report on Effective Risk Data Aggregation and Risk Reporting

Executive Summary

The Basel Committee on Banking Supervision (BCBS or "the Committee") issued a report on December 18, 2013 entitled *Progress in adopting the principles for effective risk data aggregation and risk reporting*. The publication serves as a follow-up to its January 2013 publication entitled *Principles for effective risk data aggregation and risk reporting* ("the Principles"). According to the BCBS, the fourteen Principles[1] outlined in the publication aim to strengthen risk data aggregation and risk reporting practices at banks in order to improve their risk management practices, decision-making processes, and resolvability. Firms designated as global systemically important banks (G-SIBs) are required to implement the Principles in full by the beginning of 2016.[2]

In an effort to facilitate consistent and effective implementation of the Principles among G-SIBs, the Committee decided to use a coordinated approach for national supervisors to monitor and assess the banks' progress. The first step of this approach includes issuing a "stocktaking" self-assessment survey completed by G-SIBs, other large banks, and bank supervisors during 2013. The resulting progress report provides an analysis of the G-SIBs' overall preparedness to comply with the Principles and the related implementation challenges they face, as well as some insights into the areas supervisors may potentially focus on in the coming years.

The progress report found that many banks are facing difficulties in establishing strong data aggregation governance, architecture, and processes, which represent the initial stage of implementation. To compensate, banks reported they are resorting to extensive manual workarounds. The progress report also noted that, of the thirty banks that were identified as G-SIBs during 2011 and 2012, ten reported that they will be unable to fully comply with the Principles by the 2016 deadline, citing large, ongoing, multi-year information technology and data-related projects as the main reason for their noncompliance.

[1] Of the fourteen Principles outlined in the publication, eleven Principles are designed for banks and three Principles are designed for bank supervisors.

[2] On January 16, 2014, the Office of the Comptroller of the Currency (OCC) released a proposal setting forth new standards, based on the agency's heightened expectations program, for large national banks and federal savings associations. In the proposed guidelines, the OCC stated that it expects the G-SIBs it supervises to be "largely compliant" with these Principles by the beginning of 2016. Other banks under the OCC's purview, while not expected to comply with the Principles by the beginning of 2016, should nevertheless consider the Principles to be leading practices and make an effort to bring their banks' practices into alignment with the Principles where possible.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. 33323WDC

Background

The global financial crisis that began in 2007 revealed that the information technology (IT) and data architectures of many banks were incapable of supporting the aggregation of their risk exposures and the identification of concentrations quickly and accurately across multiple dimensions, such as at the bank group level, across business lines, and between legal entities. Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices. This had severe consequences to the banks themselves and to the stability of the financial system as a whole.

To address these findings, the BCBS published the Principles on January 9, 2013, which outlined the components needed to strengthen risk data aggregation and risk reporting practices at banks in order to improve their risk management practices. The BCBS notes that, in addition to enhancing the decision-making processes of banks, improving their ability to rapidly provide comprehensive risk data by legal entity and business line will enable smoother bank resolution, thereby reducing the potential recourse to taxpayers.

The fourteen Principles, of which eleven are designed for banks and three are designed for bank supervisors, are subsets of four interrelated areas:

- *Overarching Governance and Infrastructure*, which encompasses the following two Principles*:*
  - *Governance (Principle 1):* A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other Principles and guidance established by the BCBS.
  - *Data Architecture and IT Infrastructure (Principle 2):* A bank should design, build, and maintain a data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices in both normal and stress/crisis times, while still meeting the other Principles.

- *Risk Data Aggregation Capabilities,* which encompasses the following four Principles*:*
  - *Accuracy and Integrity (Principle 3):* A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimize the probability of errors.
  - *Completeness (Principle 4):* A bank should be able to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region, and other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, concentrations, and emerging risks.
  - *Timeliness (Principle 5):* A bank should be able to generate aggregate and up-to-date risk data in a timely manner, while also meeting the Principles relating to accuracy and integrity, completeness, and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured, as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, based on the characteristics and overall risk profile of the bank.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. 33323WDC

- *Adaptability (Principle 6):* A bank should be able to generate aggregate risk data to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs, and requests to meet supervisory queries.

- *Risk Reporting Practices,* which encompasses the following five Principles:
  - *Accuracy (Principle 7):* Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.
  - *Comprehensiveness (Principle 8):* Risk management reports should cover all material risk areas within the organization. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients.
  - *Clarity and Usefulness (Principle 9):* Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand, yet comprehensive enough to facilitate informed decision-making. Reports should include meaningful information tailored to the needs of the recipients.
  - *Frequency (Principle 10):* The board and senior management (or other recipients, as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis.
  - *Distribution (Principle 11):* Risk management reports should be distributed to the relevant parties, while ensuring confidentiality is maintained.

- *Supervisory Review, Tools, and Cooperation,* which encompasses the following three Principles:
  - *Review (Principle 12):* Supervisors should periodically review and evaluate a bank's compliance with the eleven Principles above.
  - *Remedial Actions and Supervisory Measures (Principle 13):* Supervisors should have and use the appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies in its risk data aggregation capabilities and risk reporting practices. Supervisors should have the ability to use a range of tools, including Pillar 2 (the supervisory review process).[3]
  - *Home/Host Cooperation (Principle 14):* Supervisors should cooperate with relevant supervisors in other jurisdictions regarding the supervision and review of the Principles, and the implementation of any remedial action if necessary.

Although the Principles, which apply both at the group level and all material business units or entities within the group, are initially addressed to G-SIBs, the BCBS noted that national supervisors may also choose to apply the Principles to a wider range of banks. The Committee and the Financial Stability Board (FSB) are expecting G-SIBs to

[3] Please see the July 2009 Basel Committee on Banking Supervision guidance entitled *Enhancements to the Basel II framework*.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. 33323WDC

comply with the Principles by January 1, 2016. Banks designated as G-SIBs in subsequent annual updates will need to comply with the Principles within three years of their designation. Additionally, the Committee recommended that national supervisors apply the Principles to entities identified as domestic systemically important banks (D-SIBs) three years after their designation as such by their national supervisors.

Description

The BCBS and the national supervisors have agreed to monitor and assess banks' progress on complying with the Principles through the Committee's Supervision and Implementation Group (SIG), which has agreed to share its findings annually with the FSB. To facilitate consistent and effective implementation of the Principles among G-SIBs, the SIG has decided to use a coordinated approach for national supervisors to monitor and assess banks' progress until 2016. The first step of this approach includes issuing a "stocktaking" self-assessment questionnaire that was completed by thirty banks identified as G-SIBs and six other large banks during 2013. The findings from these self-assessments are outlined below.

Overall Results from the G-SIBs' Self-Assessments

The results of the self-assessment questionnaires show that, generally speaking, the Principles related to risk reporting practices scored better (i.e., had higher reported levels of compliance) than the Principles related to overarching governance and infrastructure and risk data aggregation capabilities. Banks reported the highest compliance on the following Principles related to risk data reporting: Comprehensiveness (Principle 8), Clarity and Usefulness (Principle 9), and Distribution (Principle 11).

The three Principles with the lowest reported compliance related to governance/infrastructure and data aggregation: Data Architecture and IT Infrastructure (Principle 2), Accuracy and Integrity (Principle 3), and Adaptability (Principle 6). Nearly 50 percent of the G-SIBs reported material noncompliance with these Principles and many reported that they were facing difficulties in establishing strong data aggregation governance, architecture, and processes. To compensate, banks reported they are resorting to extensive manual workarounds, which are likely to impair their risk data aggregation and reporting capabilities.

The BCBS noted, however, an anomaly in risk data reporting Principles rating higher than those related to governance/infrastructure, because governance/infrastructure Principles are "preconditions to ensure compliance with the other principles." Similarly, the Committee noted that a few banks rated themselves as fully compliant on the Comprehensiveness Principle, but materially noncompliant on one or more of the data aggregation Principles, raising a concern about the reliability and usefulness of their risk reports when the underlying data informing them and the processes to produce them have significant shortcomings.

Other Large Banks' Self-Assessments

In addition to the G-SIBs, six other large banks in four jurisdictions voluntarily participated in the questionnaire. More than half of these banks reported that they

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. 33323WDC

were largely compliant with each of the eleven Principles. None of the large banks rated themselves as fully compliant or noncompliant with any of the Principles and all but one of the banks expects to comply with the Principles by January 2016, with timeframes ranging from June 2014 to January 2016.

In general, the other large banks had slightly wider compliance gaps than the G-SIBs across all Principles, although the Committee noted that the small sample size calls for caution in drawing comparisons. The Principles and requirements related to risk reporting had higher scores for both the G-SIBs and the other large banks than the other Principles.

Supervisory Assessments

Overarching Governance and Infrastructure

Going forward, the Committee concluded that banks will need to significantly upgrade their risk IT systems and governance arrangements by putting the following in place:

- Formal and documented risk data aggregation frameworks
- Comprehensive data dictionaries that are used consistently by all group entities
- A comprehensive policy governing data quality controls
- Controls throughout the life cycle of the data.

The Committee also stressed the importance of the banks' ensuring that the role of the "data owner" is clearly documented and that accountability for the quality of risk data is established. In order to effectively support risk data aggregation and risk reporting practices, the Committee further noted that banks must also resolve the significant limitations currently affecting their risk IT systems and that banks that have not yet established their plans for independent validation of their data aggregation and reporting must make concrete efforts to do so.

Risk Data Aggregation Capabilities

The BCBS reported that banks will need to make significant efforts to improve their risk data accuracy, completeness, timeliness, and adaptability. Many banks are currently relying on manual processes that impair their ability to ensure the accuracy and timeliness of their data, particularly in stress situations such as the recent financial crisis. The BCBS noted that banks will also need to ensure that the data quality checks supporting their risk data are as robust as those supporting their accounting data.

Since Adaptability was one of the lowest-rated Principles in the risk data aggregation capabilities category, the BCBS stressed that banks will need to ensure that they can generate relevant data on a timely basis that meets evolving internal and external risk reporting requirements. Specifically, banks will need to have the following in place:

- An appropriate balance between automated and manual systems that allows for rapid aggregation of data, even in times of stress
- Documentation of timely risk data aggregation processes
- A data definition consistent across the organization
- Customization of data to users' needs.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. 33323WDC

Risk Reporting Practices

The Committee reiterated that a number of banks, when rating individual Principles, will need to take into account the interdependencies between the three areas encompassing the Principles (i.e., governance and infrastructure, risk data aggregation, and risk reporting). Specifically, within the risk data aggregation and risk reporting categories, there are Principles that are closely aligned with the intention of ensuring that compliance with the risk reporting practices is achieved through full compliance with the risk data aggregation capabilities.

Next Steps

According to the BCBS, banks have demonstrated that they understand the importance of the Principles and are committed to enhancing their data aggregation and reporting capabilities. However, each G-SIB's reported compliance status with each Principle still varies. In order to ensure that the G-SIBs will be in full compliance with the Principles by the deadline, the Committee expects that national supervisors will investigate the root causes of noncompliance and use supervisory tools or appropriate discretionary measures accordingly. The BCBS is also contemplating the following steps:

- Conducting a self-assessment survey of the banks in a reduced form and a thematic review of the requirements with the lowest scores
- National supervisors reviewing the banks' self-assessments
- Requiring that the banks stress test their ability to complete a risk data aggregation template within a limited time.

Commentary

The key weaknesses identified by the BCBS through this self-assessment exercise may provide some insight into the areas supervisors will be focusing on in the coming years:

- *Material group entities:* The report found that the self-assessment scope for many of the banks was limited to the group level and did not take into account each material business unit or entity within the group. The Committee emphasized that supervisors agree that these Principles apply not only at the group level, but also to all material business units or entities within the group.
- *Report recipients:* When providing self-ratings on the risk reporting Principles, a number of banks focused solely on the quality of risk reports to senior management and their boards, rather than including all levels of management.
- *Material risk:* The Committee found evidence that many banks assessed only a few types of risk, such as credit risk and market risk, while not comprehensively covering other types of risk, such as liquidity risk and operational risk.
- *Definitions*: Very few banks offered insights into their definitions of materiality or their tolerance level for manual versus automated processes for risk data aggregation and reporting. Some banks may have used those definitions to justify higher compliance ratings than may be warranted.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. 33323WDC

The Committee noted that these self-assessment scope limitations raise concerns that the ratings chosen by banks may not accurately reflect their compliance status in covering all material group entities, all levels of management, and all types of material risk and recommends that supervisors "closely analyze and follow up on these points during 2014."

Lastly, the inclusion of three Principles (i.e., Review, Remedial Actions and Supervisory Measures, and Home/Host Cooperation) that are directed solely at supervisory authorities underscores the importance of these data related issues to the regulatory community. Based on the results of this exercise, it is likely that supervisors will consider enhancing their efforts to: 1) fully integrate the Principles in a comprehensive way within their supervisory programs; 2) test the banks' capabilities to aggregate and produce reports in stress/crisis situations, including resolution; 3) conduct thematic reviews; and 4) develop concrete supervisory plans or other supervisory tools for 2014 and 2015.

Contact us:
This is a publication of KPMG's
Financial Services Regulatory Practice

Contributing authors:
Robert Fisher, Partner: rpfisher@kpmg.com
Christopher Dias, Principal: cjdias@kpmg.com
Brian Hart, Principal: bhart@kpmg.com
Hugh Kelly, Principal: hckelly@kpmg.com
Pamela Martin, Managing Director:
pamelamartin@kpmg.com

Earlier editions are available at:
http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/regulatory-practice-letters/Pages/Default.aspx

ALL INFORMATION PROVIDED HERE IS OF A GENERAL NATURE AND IS NOT INTENDED TO ADDRESS THE CIRCUMSTANCES OF ANY PARTICULAR INDIVIDUAL OR ENTITY. ALTHOUGH WE ENDEAVOR TO PROVIDE ACCURATE AND TIMELY INFORMATION, THERE CAN BE NO GUARANTEE THAT SUCH INFORMATION IS ACCURATE AS OF THE DATE IT IS RECEIVED OR THAT IT WILL CONTINUE TO BE ACCURATE IN THE FUTURE. NO ONE SHOULD ACT UPON SUCH INFORMATION WITHOUT APPROPRIATE PROFESSIONAL ADVICE AFTER A THOROUGH EXAMINATION OF THE FACTS OF THE PARTICULAR SITUATION.

© 2014 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International. 33323WDC