RISK DATA AGGREGATION

COMPLIANCE WITH BCBS PRINCIPLES ON RISK DATA AGGREGATION

SUMMARY

Internal auditors at banks of all sizes should be aware of the Basel Committee on Banking Supervision's regulation number 239 (BCBS 239) principles and prepare to provide assurance over their implementation and ongoing monitoring. This Financial Services Audit Center (FSAC) article provides key considerations for internal audit functions of financial institutions providing assurance over risk data aggregation based on BCBS 239 principles. It does not include an audit program, but it does include relevant engagement objectives and procedures to consider in customizing an audit program to meet the organization's needs. A future FSAC article will address BCBS 239 risk reporting principles.

Introduction

The Basel Committee on Banking Supervision (BCBS) issued Principles for Effective Risk Data Aggregation and Risk Reporting in January 2013 in response to the global financial crisis of 2007 to 2009. Known as BCBS 239, the purpose of this guidance is to reduce the probability of another global crisis through improving banks' risk management practices, decision-making processes, and resolvability.

The Basel Committee expected globally systemically significant banks (G-SIBs) to be in compliance with BCBS 239 by January 2016, and the committee expects domestic systemically important banks (D-SIBs) to be in compliance within three years after their designation as such.

Supervisors of various jurisdictions are likely to draw from BCBS 239 as they conduct their bank exams; therefore, internal auditors should be aware of the principles and prepare to provide assurance over their implementation and ongoing monitoring.

Overview of BCBS 239

BCBS 239 is organized into 14 principles, which are further divided into four closely related topics: 1) overarching governance and infrastructure, 2) risk data aggregation capabilities, 3) risk reporting practices, and 4) supervisory review, tools, and cooperation (Exhibit 1). The complete guidance is available from the Bank for International Settlements (BIS) at www.bis.org.[1]

This Financial Services Audit Center (FSAC) article summarizes the requirements of BCBS 239, provides an overview of the Basel Committee's 2017 progress report on the adoption of principles, and gives key considerations for providing assurance over principles for risk data aggregation. A future FSAC article will address assurance over the risk reporting principles.

2017 Progress Report Overview

According to the Basel Committee's March 2017 report, only one G-SIB had fully implemented the principles, and "substantial work" still needs to be done by banks to achieve compliance. (See "Progress in Adopting the Principles for Effective Risk Data Aggregation and Risk Reporting" at www.bis.org.)

[1] Established on May 17, 1930, the Bank for International Settlements (BIS) is an international financial organization owned by 60 member central banks, representing countries from around the world that together make up about 95 percent of world GDP.

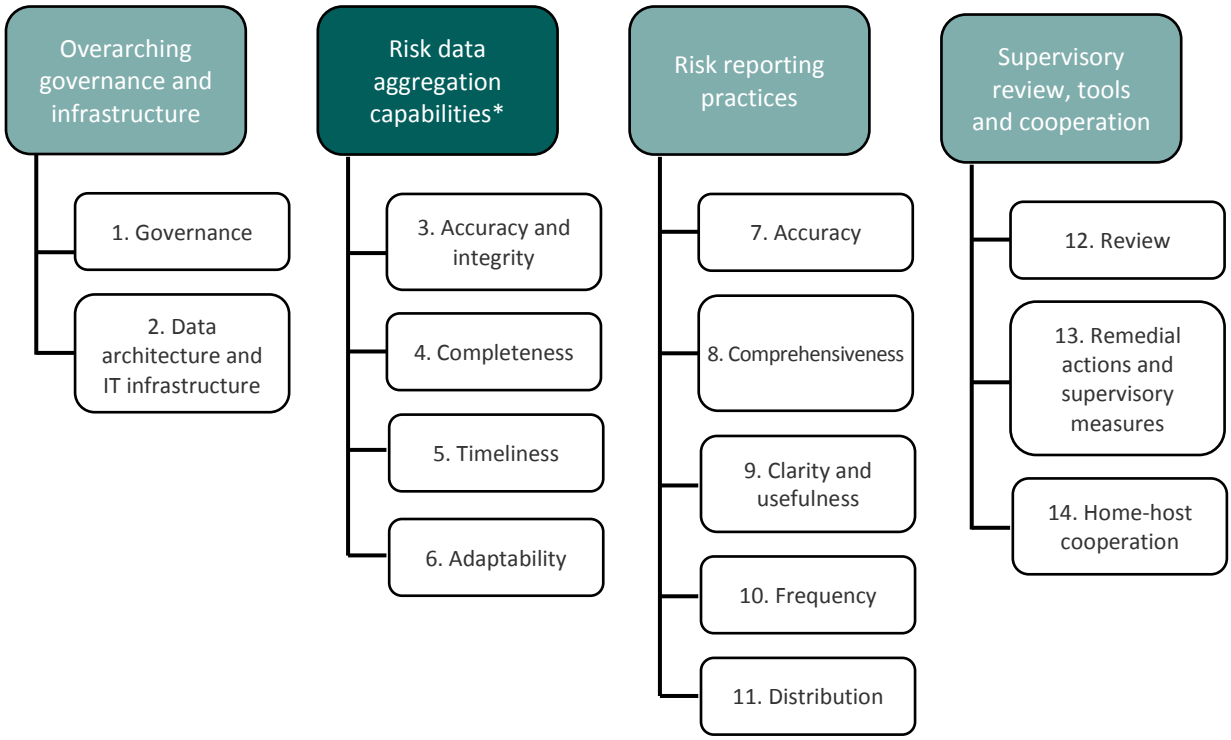
The 2017 progress report provides a valuable indication of the supervisory focus that other banking institutions may experience. According to the report, the average compliance rating by Principle ranged from 2.60 to 3.37 on a four point scale. Supervisors across the banking industry may focus on assessing compliance with the lowest rated principles and push for improvements. At the same time, supervisors may expect existing compliance with highest rated principles. Internal audit should provide assurance that banks are already strong in those areas. Supervisors have recommended "increasing the scope and quality of validation by internal audit" as a measure to address non-compliance.

The major technical challenges that supervisors observed were difficulties in managing large-scale IT projects, overreliance on manual processes to produce risk reports, incomplete implementation of data architecture, and weaknesses in data quality controls.

Banks also struggled to determine materiality thresholds that supervisors would find acceptable. As defined in the Principles, the concept of materiality means that risk management data and reports can exclude information only if the information "does not affect the decision-making processes in banks." During a recent supervisory review, internal audit was asked to "review the adequacy of the definition of materiality;" therefore, internal auditors should prepare to address this issue.

The Basel Committee urged banks to view implementation of the principles as a dynamic and ongoing process. For example, whenever banks pursue new initiatives or make changes in their business models or risk profiles, they should consider risk data aggregation and risk reporting (RDARR) requirements. In addition, banks should have processes to detect and monitor emerging trends through forward-looking forecasts and stress tests. Finally, IT systems, policies, and processes need to be periodically assessed and improved to be able to maintain compliance with the Principles.

Exhibit 1: Summary of the BCBS 239 Principles



Source: Principles for Effective Risk Data Aggregation and Risk Reporting (Basel Committee on Banking Supervision, January 2013). Available at www.bis.org. * This FSAC article addresses principles 3–6. A future article will address principles 7–11.

Providing Assurance over Risk Data Aggregation Capabilities

Risk data aggregation is described by BCBS 239 as "defining, gathering, and processing risk data according to the bank's risk reporting requirements to enable the bank to measure its performance against its risk tolerance/appetite. This includes sorting, merging, or breaking down sets of data." The Principles for risk data aggregation address the areas of accuracy and integrity, completeness, timeliness, and adaptability. In the sections that follow, considerations for providing assurance over each of the risk data aggregation principles are provided.

According to IIA Standard 2110: Planning, the CAE must establish a risk-based internal audit plan — that plan will likely include engagements to provide assurance over the bank's risk data aggregation capabilities and performance. In addition, all engagements must be performed with due professional care. The scope of the engagement should include identifying relevant systems, records, personnel, and physical properties (including those under the control of third parties). As part of the engagement, internal auditors must document sufficient, reliable, relevant, and useful information to support the findings related to risk data aggregation (IIA Standard 2330). Finally, the results of the engagement must be communicated (IIA Standard 2400). Audit reports should communicate whether the bank appropriately defines and applies the concept of materiality, as defined in BCBS 239, i.e., information that would "affect the decision-making processes in banks."

Specific considerations for identifying information (IIA Standard 2310) and analysis and evaluation (IIA Standard 2320) are described below for each Principle.

Principle 3: Accuracy and Integrity

Principle 3: Accuracy and Integrity – 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.

Audit Focus

IIA Standard 2010: Planning

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

IIA Standard 1220: Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1220.A2: In exercising due professional care internal auditors must consider the use of technology-based audit and other data analysis techniques.

IIA Standard 2330: Documenting Information

Internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.

IIA Standard 2400: Communicating Results

Internal auditors must communicate the results of engagements.

IIA Standard 2310: Identifying Information

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

IIA Standard 2320: Analysis and Evaluation

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

Data accuracy and integrity is largely dependent on the quality of data. Examples of proper data quality controls include appropriate data element certification, data quality documentation, data quality assurance mechanisms, assessment of data quality per risk type, and documented and effective controls for manual processes. According to the 2017 progress report, banks achieved the *lowest* level of compliance with Principle 3. Internal auditors should be prepared for supervisors to examine this area closely.

Relevant Internal Audit Engagement Objectives

- **Accuracy.** Provide assurance that the bank can meet normal and stress/crisis reporting accuracy requirements. Banks should have clear documentation of risk data aggregation processes, an enterprise-wide data taxonomy, and reconciliation of data between different sources.
- **Integrity.** Provide assurance that mitigants and controls for manual processes effectively minimize the probability of errors, and provide assurance that there is appropriate balance between automated and manual systems.
- **Overall Assessment.** Assess the progress toward compliance with Principle 3 overall and estimate expected date of full compliance.

Relevant Internal Audit Engagement Procedures

Reconciliation. Identify bank sources that can be reconciled against risk data for accuracy, for example, accounting data. Determine whether there is a lack of reconciliation for key reports. Provide assurance that the organization is consistently following and monitoring a formalized data reconciliation framework, which includes a rationale for differing methodologies and results should they exist. Data quality standards should be mapped and integrated across the enterprise, including overseas subsidiaries. Data quality rules should be properly established, for example, with minimum standards for data quality reporting thresholds.

Manual Processes. Identify whether manual processes for risk data aggregation exist. If manual processes exist, identify the governing policies and procedures. Provide assurance that controls for manual processes (including a data amendment policy) are documented and effective to protect the accuracy and integrity of the aggregated risk data. Propose appropriate options to automate processes wherever possible.

Authoritative Source. Identify the authoritative source (if any) for each type of risk data (as documented in organizational policies and procedures). Evaluate the quality of the authoritative sources. Provide assurance that a designated authority exists to oversee the effectiveness of data quality rules and reporting frameworks developed by local risk functions.

Access. Identify documentation related to personnel's access to appropriate risk data. Evaluate the processes and systems to provide assurance that personnel have appropriate and timely access to risk data. If there are overseas subsidiaries, provide assurance that risk data is accessible.

Data Taxonomy. Determine whether the bank has established a data taxonomy. Evaluate the quality, completeness, and consistency of use for the enterprise-wide data taxonomy. If no taxonomy exists, evaluate the impact on risk data accuracy and integrity.

Documentation. Verify that documentation exists for all risk data aggregation processes (both automated and manual). Validate that documentation is complete. In particular, any manual workarounds should be documented with an explanation of their appropriateness, a description of their criticality to the accuracy of risk data aggregation, and proposed actions to reduce the impact.

Monitoring and Escalating. Verify that banks have a process in place to continuously measure, monitor, escalate, and rectify data accuracy and integrity issues. Evaluate the effectiveness of processes in place to measure, monitor, escalate, and rectify data accuracy and integrity issues. In particular, provide assurance that variance analysis is in place to determine if there are any changes in reports over time. Banks should also be able to make timely adjustments of risk data aggregation methods and procedures in response to business development, risks, and regulatory changes.

Principle 4: Completeness

Principle 4: Completeness – 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.

Completeness is measured in terms of whether all material risk data can be aggregated. BCBS 239 defines materiality as information that would affect the decision-making processes in banks. In applying the materiality concept, banks need to consider the "size of the exposures concerned, types of risk involved, and the dynamic nature of the banking business." In addition, banks should be able to analyze the data by groups that are relevant to the risk in question, for example, business lines, legal entities, asset types, industries, regions, and other groups.

Relevant Internal Audit Engagement Objectives

- **Materiality.** Determine the definition of materiality for risk data aggregation and risk reporting that has been established by the bank's board and senior management.
- **Completeness.** Provide assurance that all material risk data can be aggregated across the entity.
- **Analysis by Group.** Provide assurance that data is available by groups that would be relevant for the risk in question.
- **Overall Assessment.** Assess the progress toward compliance with Principle 4 overall and estimate expected date of full compliance.

Relevant Internal Audit Engagement Procedures

Material Risk Exposures. Identify all material risk exposures for the enterprise, including those that are off-balance sheet. Provide assurance that the bank can explain its chosen definition of materiality to supervisors and that risk data aggregation capabilities are adequate for all material risk exposures, including those that are off-balance sheet.

Aggregation Systems. Identify the risk aggregation systems in place and locate the documentation that describes the specific approach used by each system to aggregate exposures for any given risk measure. Provide assurance that risk data aggregation capabilities are at equal levels regardless of which system is being used for aggregation. Finally, verify that the specific aggregation approach used by each system is clearly documented.

Completeness. Identify which risk data must be aggregated in order for material risk exposures to be addressed completely. Identify how the completeness of the aggregated risk data is measured and monitored. Provide assurance that the completeness of risk data is measured and monitored and be able to identify and explain any material exceptions.

Principle 5: Timeliness

Principle 5: Timeliness – 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, set based on the characteristics and overall risk profile of the bank.

Timeliness of risk data aggregation is essential in order for banks to have data at the right time for decision-making. Timeliness also addresses the need to produce data quickly in response to stress/crisis situations. To assess banks' abilities to respond in a timely manner to ad-hoc risk data requests, some supervisors have explored the use of fire drills. In these cases, supervisors have used the banks' internal audit functions to validate, or certify, the completeness and accuracy of data produced in response to the supervisors' requests.

Relevant Internal Audit Engagement Objectives

- **General Timeliness.** Provide assurance that the bank can generate up-to-date risk data and aggregate it in a timely manner, under both normal and stress/crisis situations.
- **Risk-based Timeliness.** Provide assurance that risk data can be aggregated at a speed that is appropriate for the nature and potential volatility of the risk being measured and its criticality to the overall risk profile of the bank.
- **Frequency Requirements.** Provide assurance that bank-specific frequency requirements for aggregating risk data are followed and are adequate to produce up-to-date risk data in a timely manner, under both normal and stress/crisis situations.
- **Overall Assessment.** Assess the progress toward compliance with Principle 5 overall and estimate expected date of full compliance.

Relevant Internal Audit Engagement Procedures

Reporting Requirements. Determine the risk management reporting requirements first, and then determine what aggregate risk information is needed to produce those reports. Provide assurance that risk data aggregation capabilities are able to produce aggregate risk information on a timely basis to meet reporting requirements.

Data for Critical Risks in Stress/Crisis Situations. Identify enterprise-specific critical risks first, and then identify what risk data may be needed rapidly in a stress/crisis situation for these critical risks. Provide assurance that risk systems can produce aggregated risk data on a timely basis for critical risks during times of stress/crisis.

Frequency Requirements. Identify the frequency requirements the bank has set for aggregating risk data. Provide assurance that the frequency requirements are followed and are adequate to generate aggregate and up-to-date risk data in a timely manner, under both normal and stress/crisis situations.

Principle 6: Adaptability

Principle 6: Adaptability – 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 data aggregation capabilities need to be adaptable enough to respond to on-demand, ad hoc requests that may require data in a form that is different than what is required by routine risk data reports. These capabilities are especially critical during stress/crisis situations. Banks also need the ability to aggregate risk data in new ways to respond to changing internal needs and to meet supervisory queries.

Relevant Internal Audit Engagement Objectives

- **On-demand, Ad Hoc Data Aggregation.** Provide assurance that the bank can generate aggregate risk data to meet on-demand, ad hoc risk management reporting requests.
- **Overall Assessment.** Assess the progress toward compliance with Principle 6 overall and estimate expected date of full compliance.

Relevant Internal Audit Engagement Procedures

Flexibility and Adaptability. Determine which processes and procedures are in place to aggregate data for on-demand and ad hoc data requests. Provide assurance that processes and procedures are flexible and can be executed quickly. Data customization options should include drill downs and the ability to produce quick summary reports. In addition, data aggregation systems should be updated as appropriate in response to new developments that affect the bank's risk profile. Finally, data aggregation systems should be adaptable to accommodate changes in regulatory frameworks.

Data Subsets. Identify data subsets relevant to material risk exposures and determine the systems in place to produce the data subsets. Provide assurance that data subsets can be aggregated quickly. Subsets that may

need to be aggregated include country credit exposures, date ranges, industry types, business lines, and geographic areas.

Conclusion

Internal audit has an opportunity to be a trusted advisor to executive management and the board by providing continuous assurance over the bank's compliance with each of the 14 BCBS Principles. Implementation of internal audit's recommendations should help banks improve risk data aggregation and reporting processes, leading to better decision-making. Supervisors at various levels are likely to expect internal audit functions to provide assurance over implementation efforts as well as ongoing monitoring of compliance.

Finally, as appropriate risk data aggregation processes are being established, internal audit must also consider the effectiveness of risk reporting. Key considerations for providing assurance over BCBS Risk Reporting Principles will be addressed in a future FSAC article.

Potential Strategies for Compliance with Risk Data Aggregation Principles

The Basel Committee suggested the following strategies for compliance with Principles 3–6:

- Develop IT infrastructure to aggregate a broader range of risk data automatically and reduce reliance on manual workarounds.
- Automate data quality controls and improve reporting capabilities associated with group-wide stress testing.
- Improve systems to monitor and enforce credit limits status across risk types and products.
- Promote data alignment between risk and finance, using common data dictionaries and appropriate governance structure.
- Establish data collection channels, processes, and procedures that encompass the development of common taxonomies and reference data so as to facilitate data aggregation in times of stress/crisis.
- Enhance data aggregation capabilities to consolidate data from branches and subsidiaries operating in other jurisdictions and, more generally, develop consolidated data stores, notably for credit, market, and operational risks to expedite risk reporting and easier reconciliation of risk data.
- Implement programs aimed at meeting Basel III regulatory requirements and other international initiatives (e.g., Legal Entity Identifiers).
- Provide appropriate access to sufficient staff with expert knowledge of risk control functions and data so they are able to process ad-hoc data report requests.

Source: Progress in Adopting the Principles for Effective Risk Data Aggregation and Risk Reporting (Basel Committee on Banking Supervision, January 2015). Available at www.bis.org.

About the Financial Services Audit Center

Established in 2015, the Financial Services Audit Center (the Center) is a specialty offering of The IIA for financial services auditors. The Center was established to provide financial services auditors with low-cost, high-quality professional development; networking opportunities for knowledge sharing among financial services stakeholders; and ongoing, timely, and relevant reporting on trends, benchmarking, and thought leadership in the audit profession.

About The IIA

Established in 1941, The IIA is an international professional association with global headquarters in Lake Mary, Fla., USA. The IIA is the internal audit profession's international standard-setter, sole provider of globally accepted certifications, and principal researcher and educator.

Disclaimer

The Center and The IIA publish this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The Center and The IIA recommend that you always seek independent expert advice relating directly to any specific situation. The Center and The IIA accept no responsibility for anyone placing sole reliance on this material.

Financial Services
AUDIT CENTER

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746-5402, USA

Phone: +1-407-937-1111

Fax: +1-407-937-1101

www.theiia.org/FSAC