RISK REPORTING PRACTICES

COMPLIANCE WITH BCBS 239 PRINCIPLES FOR RISK REPORTING PRACTICES

Introduction

Note: This is the second Knowledge Brief on BCBS 239: Principles for effective risk data aggregation and risk reporting. A prior Knowledge Brief addressed BCBS 239 principles for risk data aggregation.

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 BCBS expected globally systemically important 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.

Risk reporting is one of four major areas addressed in BCBS 239, along with risk data governance, risk data aggregation, and supervisory review. As large banks take steps to implement the Principles, internal auditors at banks of all sizes may be expected to provide assurance over the implementation process and ongoing compliance.

According to BCBS 239, effective risk reporting must be forward looking and serve as an early warning system for potential breaches of risk limits.

SUMMARY

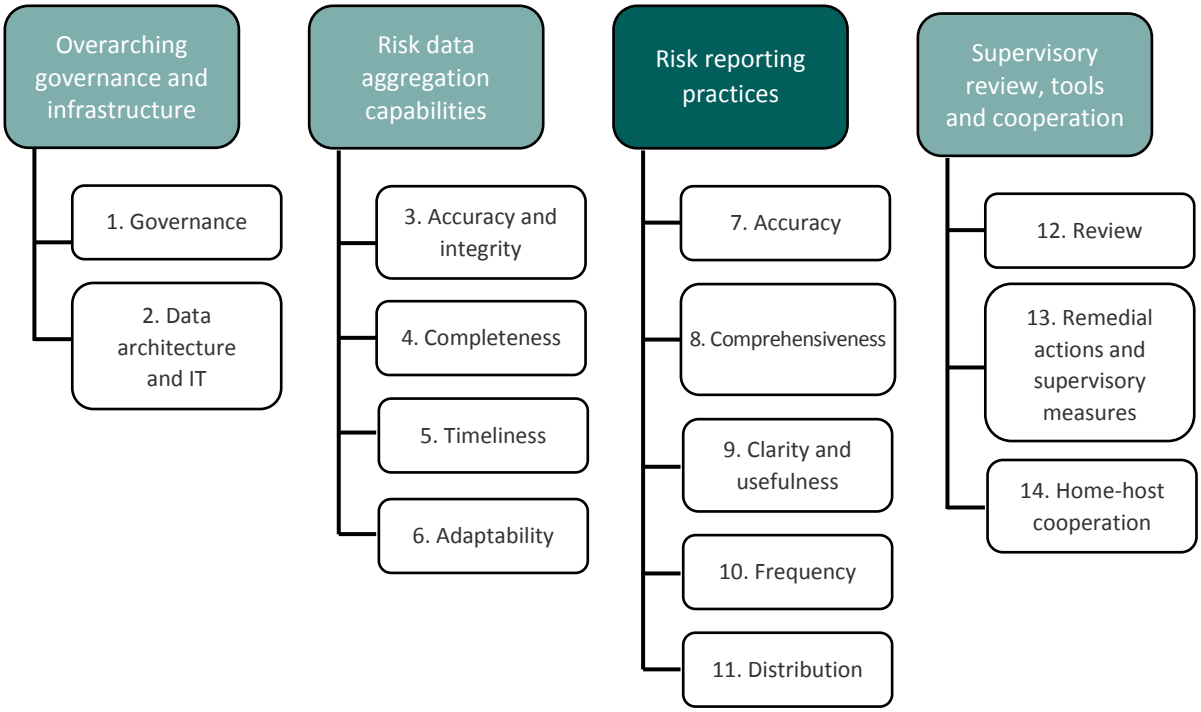
To manage risk effectively, the right people need the right information at the right time. Risk reporting is one of the key areas addressed in BCBS 239, issued by the Basel Committee on Banking Supervision. This article offers relevant engagement objectives and procedures to consider in customizing an audit program to review risk reporting practices.

This Financial Services Audit Center (FSAC) article summarizes the requirements of BCBS 239, provides an overview of the Basel Committee's 2017 report Progress in adopting the *Principles for effective risk data aggregation and risk reporting* (2017 Progress Report), and gives key considerations for providing assurance over the principles for risk reporting practices. A prior FSAC article addressed assurance over the risk aggregation principles.

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).

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 Knowledge Brief addresses principles 7–11. A prior Knowledge Brief addressed principles 3–6.

2017 Progress Report Overview

According to the 2017 Progress Report, only one G-SIB had fully implemented the Principles, and "substantial work" still needs to be done by banks to achieve compliance.

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 BCBS 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.

Audit Focus

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.

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.

2220: Engagement Scope

The established scope must be sufficient to achieve the objectives of the engagement.

> **2220.A1:** The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under control of third parties.

2310: Identifying Information

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

2320: Analysis and Evaluation

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

2330: Documenting Information

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

2400: Communicating Results

Internal auditors must communicate the results of engagements.

Finally, IT systems, policies, and processes need to be periodically assessed and improved to be able to maintain compliance with the Principles.

Applicable IIA Standards

IIA *Standards* provide a flexible and adaptable framework for providing assurance over risk reporting capabilities and performance. When the risk-based internal audit plan is developed, it will likely include engagements for risk reporting (IIA Standard 2010: Planning). If the engagement is conducted in conformance with IIA *Standards*:

- Appropriate use of technology will be applied to the engagement as part of due professional care (IIA Standard 1220.A2).
- The scope of the engagement will include relevant systems, records, personnel, and physical properties, including those under the control of third parties (IIA Standard 2220.A1).
- Sufficient, reliable, relevant, and useful information will be documented to support the findings (IIA Standard 2330: Documenting Information).
- The results of the engagement will be communicated to the appropriate parties (IIA Standard 2400: Communicating Results).

For each risk reporting principle, internal audit should confirm that:

- Processes and procedures have been established with appropriate controls.
- Processes and procedures are adequate to meet objectives.
- Processes and procedures are being followed.

Processes are expected to provide a high-level overview, while procedures should provide details about the functional execution of tasks.

Providing Assurance Over Risk Reporting Practices

According to BCBS 239, "To manage risk effectively, the right information needs to be presented to the right people at the right time. Risk reports based on risk data should be accurate, clear, and complete. They should contain the correct content and be presented to the appropriate decision-makers in a time that allows for an appropriate response."

The principles for risk reporting practices address accuracy, comprehensiveness, clarity and usefulness, frequency, and distribution. According to the 2017 Progress Report, banks achieved their highest levels of compliance with the principles for risk reporting practices — receiving an average rating of largely compliant for three of the five Principles: Principle 8 (comprehensiveness), Principle 9 (clarity and usefulness), and Principle 11 (distribution).

To provide assurance over the organization's risk reporting practices, internal audit should review risk management reports to the board, senior management, and staff, and determine whether content, granularity, and frequency are appropriate. Relevant internal audit engagement objectives and procedures to consider in providing assurance over each principle follow. However, engagement objectives and procedures should be customized to meet the needs of the organization.

Principle 7: Accuracy

> **Principle 7: Accuracy** – Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.

According to BCBS 239:

- Accuracy is the "closeness of agreement between a measurement or record or representation and the value to be measured, recorded, or represented."
- Precision is the "closeness of agreement between indications or measured quantity values obtained by replicating measurements on the same or similar objects under specified conditions."

Relevant Internal Audit Engagement Objectives

The internal audit activity will provide assurance over the following:

- **Confidence in Risk Reporting.** The board and senior management have a high degree of confidence in the accuracy and precision of critical risk.
- **Processes and Procedures.** Processes and procedures for ensuring accuracy of risk reporting are operating as intended.
- **Approximations.** The bank has established reasonable expectations for the reliability of approximations.
- **Accuracy and Precision Requirements.** Senior management has established adequate accuracy and precision requirements.
- **Materiality.** The bank has adequately considered materiality in its established rationale for accuracy requirements.
- **Overall Assessment.** The bank is in full compliance with Principle 7 by expected date.

Relevant Internal Audit Engagement Procedures

Assess the level of confidence among the board and senior management in the risk information they are provided. Are they using the risk information to make critical decisions about risk?

Verify that appropriate processes and procedures are in place so that risk reporting is accurate. At a minimum, BCBS 239 calls for banks to maintain:

- Requirements and processes to reconcile reporting to risk data.
- Editing and reasonableness checks (both automated and manual).
- Validation rules for quantitative information (with explanations of their logic).
- Exception reports that explain data errors or weaknesses in data integrity.

Identify expectations set by the bank for the reliability of approximations, including results from models, scenario analysis, and stress testing. **Verify** that BCBS 239

principles for risk reporting and data quality are applied to approximations.

Identify requirements set by senior management for accuracy and precision of risk reporting. **Determine** whether requirements take into consideration the criticality of decisions based on the information. **Determine** whether requirements are customized for regular and stress/crisis reporting.

Assess whether accuracy requirements are aligned with the concept of accounting materiality, i.e., an inaccuracy is unacceptable if it could influence the risk decisions of users. In addition, the bank should have a rationale to support its accuracy requirements. For reconciliation requirements, **verify** that standards are based on validation, testing, or reconciliation results.

Principle 8: Comprehensiveness

> **Principle 8: Comprehensiveness** – 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.

Comprehensiveness requires appropriate depth of scope of information, with an emphasis on proactive and dynamic analysis. For example changing economic conditions or risks should be identified. Forecasts and forward-looking stress tests should be a standard part of risk reporting.

Relevant Internal Audit Engagement Objectives

The internal audit activity will provide assurance over the following:

- **Exposure and Position Information.** Risk reporting includes exposure and position information for all significant risk areas.
- **Emerging Risks and Trends.** Emerging issues are monitored in risk reports and recommendations for action are proposed as needed.
- **Risk Report Components.** Components included in risk reports are material and complete.
- **Forward-looking Assessment of Risk.** The risk reports contain forecasts and scenarios for the bank's capital and risk profile in the future.
- **Overall Assessment.** Full compliance with Principle 8 by expected compliance date.

Relevant Internal Audit Engagement Procedures

Identify the organization's significant risk areas (e.g., credit, market, liquidity, operational). Within these risk areas, **identify** significant components (e.g., single name, country, industry). Finally, **identify** risk-related measures that may also be needed (e.g., regulatory or economic capital). **Verify** that these components are included in risk reporting.

Verify that the aggregated risk reporting includes the information required by Principle 8, paragraph 59, including, but not limited to, capital adequacy, regulatory capital, capital and liquidity ratio projections, credit risk, market risk, operational risk, liquidity risk, stress testing results, inter- and intra-risk concentrations, and funding positions and plans.

Assess whether risk reporting adequately addresses:

- Emerging risk concentrations.
- Status of measures to deal with specific risk situations.
- Forward-looking forecasts and stress tests.
- Forecasts or scenarios for key market variables and their effects on the bank.

Principle 9: Clarity and Usefulness

> **Principle 9: Clarity and Usefulness** – 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.

BCBS 239 describes clarity and usefulness as risk reports that should be "easily understood and free from indistinctness or ambiguity." Principle 9 takes into consideration differing information needs of the board,

senior management, and other levels of the organization. To be useful, reports need an appropriate balance between data, discussion, explanation, and recommended conclusions.

Relevant Internal Audit Engagement Objectives

The internal audit activity will provide assurance over the following:

- **Recipient Requirements.** The board and senior management are requesting and receiving risk reports that meet their requirements.
- **Risk Data Inventory.** The bank has established a sufficient inventory and classification of risk data items.
- **Balance.** There is adequate balance between data, analysis, discussion, explanation, and conclusions provided in reports.
- **Report Recipient Feedback.** Risk report recipients provide recorded confirmation that information is relevant, appropriate, and received periodically.
- **Overall Assessment.** Full compliance with Principle 9 by expected compliance date.

Relevant Internal Audit Engagement Procedures

Identify all aggregated risk reports and determine the primary recipients for each one (board, senior management, etc.).

Assess the information in the reports for appropriate balance between data reporting, quantitative analysis, qualitative analysis, interpretation, and recommended conclusions. As noted in the 2017 Progress Report, effective reports have a clear focus and specific items have been highlighted for attention or action.

To assess the usefulness of reports, **verify** that report recipients (such as the board and senior management) periodically confirm that the information aggregated and reported is "relevant and appropriate, in terms of both amount and quality, to the governance and decision-making process" (BCBS 239, paragraph 69).

Verify that boards, senior management, and other report recipients have established reporting requirements.

Clarity and usefulness requirements also apply to ad hoc or crisis reporting. **Verify** that procedures are in place to produce clear and useful reports under these conditions and **confirm** that reports are effectively tailored to the needs of specific recipients.

Taking into consideration the overall impetus for risk reporting to be forward-looking, **determine** whether there is appropriate balance between static reporting and dynamic reporting (such as live dashboards).

Verify that risk reporting processes utilize standard terms, glossaries, or data dictionaries, focusing on concepts such as taxonomy, data classification, and metadata. **Assess** the effectiveness of the inventory or classification of risk data items used in reporting.

Principle 10: Frequency

> **Principle 10: Frequency** – 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.

The frequency of reporting should be based on requirements for information needed to make sound decisions. Frequency should be increased during times of stress/crisis. An overreliance on manual processes can impede a bank's ability to produce reports with appropriate frequency, especially in response to ad hoc requests or during crisis/stress situations, and should be corrected.

Relevant Internal Audit Engagement Objectives

The internal audit activity will provide assurance over the following:

- **Speed of Reporting.** Requirements are established for how quickly each report needs to be produced both in normal and stress/crisis situations.
- **Stress/Crisis Situations.** Reports can be produced in very short time periods.

- **Overall Assessment.** Full compliance with Principle 10 by expected compliance date.

Relevant Internal Audit Engagement Procedures

Verify that the bank periodically assesses requirements for how quickly reports need to be produced, based on the purpose of each report and the speed at which risk can change. Reporting frequency should be higher during times of stress/crisis than during normal times.

Verify that the bank routinely conducts tests to examine its ability to rapidly produce reports in crisis/stress situations, including intraday reporting as appropriate.

Principle 11: Distribution

> **Principle 11: Distribution** – Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained.

A lack of timely and confidential distribution to relevant parties could undermine the effectiveness of the risk reporting process. Distribution effectiveness must be confirmed periodically.

Relevant Internal Audit Engagement Objectives

The internal audit activity will provide assurance over the following:

- **Recipients.** Appropriate recipient lists are in place and periodically reviewed for each report.
- **Confidentiality.** Confidentiality measures for risk reports are effective.
- **Confirmation of Receipt.** The appropriate individuals in the distribution plan are receiving reports as intended.
- **Overall Assessment.** Full compliance with Principle 11 by expected compliance date.

Relevant Internal Audit Engagement Procedures

Verify that appropriate report recipient lists are in place for each report. **Verify** that those on report recipient lists are contacted periodically to confirm that they have received reports. **Validate** those confirmations.

Verify that procedures are in place to distribute reports in a timely manner.

Verify that confidentiality and report access controls such as data confidentiality agreements, and policies governing the use of secured media, collaborative workspaces and encrypted emails, are in place.

Closing Thoughts

On average, banks reached higher levels of compliance with BCBS 239 principles for risk reporting practices than with BCBS 239 risk data aggregation principles. However, banks on average still fell short of being largely compliant with Principle 7 (Accuracy) and Principle 10 (Frequency).

Through assurance services, internal auditors can help banks to achieve full compliance with BCBS 239 — but achieving full compliance is only part of the value proposition. By providing assurance over risk aggregation and reporting practices — and related recommendations derived from sound collaboration with key business partners — internal audit can help risk management functions strengthen the integrity of risk reports leading to better decision-making throughout the organization.

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

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla. For more information, visit www.theiia.org.

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.

Copyright

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