

IMPROVING YOUR RISK DATA AGGREGATION (RDA)

PLANNING AHEAD FOR BCBS 239 COMPLIANCE

By Matt McGivern, managing director, Business Intelligence & Data Governance, Protiviti

The global financial crisis exposed that many banks did not have an adequate understanding of the data architecture and technology used to manage their financial risks. As a result, the warning signs of the meltdown were not pieced together until it was too late.

To help prevent a repeat of this scenario in the future, the Basel Committee on Banking Supervision (BCBS) issued regulation 239: Principles for Effective Risk Data Aggregation and Risk Reporting. These 14 principles are organized into four topic areas: 1) overarching governance and infrastructure, 2) risk data aggregation capabilities, 3) risk reporting practices, 4) supervisory review, tools, and cooperation.

This article focuses on:

- The role of internal audit in risk data aggregation (RDA).
- How to prepare for compliance with BCBS 239.
- Best strategies for data governance.

What Is Risk Data Aggregation (RDA)?

At its core, RDA simply means organizing your data about risk so that you can use it effectively. This activity includes:

- Defining your data.
- Capturing and reporting both technical and business metadata.
- Organizing metadata within systems.
- Accessing and reporting data as needed.
- Combining business knowledge with key data in order to measure and manage risks.
- Providing this data to the right business processes and end users for decision-making.

SUMMARY

In the wake of the financial meltdown that started in 2007, regulators are paying increased attention to data governance. Learn about:

- The role of internal audit in risk data aggregation (RDA).
 - How to prepare for compliance with BCBS 239.
 - Best strategies for data governance.
- Protecting the overall integrity and quality of the data.

Challenges for BCBS 239 Compliance

Thirty-one Globally Systemically Important Banks (G-SIBs) have periodically completed self-assessments of their overall progress toward BCBS 239 compliance.¹ The most recent results were published in January 2015. For the topic areas of risk data aggregation and risk reporting, the highest levels of noncompliance were related to principles 2, 3, and 6:

Principle #2: Data Architecture & IT Infrastructure

- 77 percent were materially noncompliant on integrated data taxonomies and glossaries.
- 40 percent were materially noncompliant on data production and control across the data lifecycle.

Principle #3: Accuracy & Integrity [of Data]

- 57 percent were materially noncompliant on their documentation of risk data aggregation processes.
- 60 percent were materially noncompliant on their level of dependency on manual data reconciliation processes.

GETTING TO KNOW YOUR DATA

Risk data aggregation (RDA) involves technical, business, and risk metadata. (Metadata is a set of data that describes and gives information about other data.) Here are the key components of each type of metadata:

- **Technical Metadata.** Information about where data comes from, the data type (e.g. number, currency, text), physical database locations, and other technical details required to locate and query data sets.
- **Business Metadata.** Glossary of how the data points are leveraged within key business processes to generate value, including the potential “fit for use” of specific data elements, business rules used for calculated or generated fields, and, potentially, ownership of the data within the business.
- **Risk Metadata.** Definitions of specific risks each data element might be tied to, including how it should be combined with other elements, calculated, or modeled to properly articulate specific risks. For RDA this covers all different types of risks across the organization, including, but not limited to, credit, market, liquidity, operations, and other risk areas.

Principle #6: Adaptability

- 43 percent are materially noncompliant on the customization of data.

Financial institutions should take a closer look at these principles to prepare for compliance requirements.

Getting Ready for Compliance

The BCBS 239 principles call for periodic validation, stating, “This validation should be independent and review the bank’s compliance with the principles in this document.”²

The initial compliance deadline of January 1, 2016, was for G-SIBs only. Even though compliance is not yet required for smaller financial institutions, regulators are paying increased attention to data governance, in particular when viewing the data they receive from firms responding to compliance reporting.

In addition, BCBS 239 calls for reviewers to have skills and qualifications necessary to effectively conduct these reviews: “[Reviews] should be conducted using staff with specific IT, data, and reporting expertise.”³

Data expertise is an area where internal auditors feel a need for improvement. According to Protiviti’s 2016 Internal Audit Capabilities and Needs Survey, internal auditors in financial services ranked “data analysis tools—statistical analysis” as the area needing most improvement for audit process knowledge.⁴ Internal auditors in financial services should expect the importance of technical expertise to grow.

Best Strategies for Data Governance

How can internal auditors prepare to come into compliance on the three most challenging principles from BCBS 239: data infrastructure, accuracy and integrity of data, and adaptability for risk reporting?

The key is to establish and support effective data governance throughout the organization. Here are the basic data governance strategies that need to be established and maintained:

Break Down Data Silos. Enforce enterprise-wide data governance strategies and processes, which will help to tear down data silos and enable a free flow of data within the enterprise.

Establish Proper Data Architecture. Invest in the underlying data architecture to limit data redundancy; ensure business rules are applied uniformly and with transparency; and provide better input, processing, and output controls for source systems of data.

Understand Source Data and Coverage. Enforce effective master and reference data management programs, which will enable the institution to uncover data structure issues. In the event of data unavailability, establish processes to source data such that downstream RDA processes can effectively leverage the dataset and perform a more refined data analysis.

Maintain Metadata. Enable a centralized repository of metadata, which will allow the institution to recognize redundant data processes and identify others that can be deprecated thus reducing total cost of ownership of various data sourcing applications. As noted before, metadata may include technical, business, and risk attributes within the same repository.

Enhance Ad Hoc and Reporting Capabilities. Provide end-users with access to quality, well-defined data sets to satisfy everyday reporting needs and ad hoc requests.

Conclusion

Overall, we are just starting the journey on BCBS 239, with G-SIBs already compelled and D-SIBs (domestic systemically important banks) preparing for compliance. Internal audit will play a key role in verifying the effectiveness of risk data reporting, including opining on the underlying data infrastructures and risk aggregation processes. This involvement will require varied skills, including infrastructure, processes, and business knowledge required to align the BCBS 239 demands against the internal capabilities delivering the RDA results.

ABOUT THE AUTHOR

Matt McGivern is a managing director in the Business Intelligence and Data Governance Group within global consulting firm Protiviti. He has more than 20 years of experience in information technology, financial services, and project management. He has worked in professional services for the last 17 years, focusing on data warehousing, financial and management reporting, project management, and full lifecycle software development. He has also completed major projects focused on financial and management reporting, business intelligence, and general management consulting.

Notes

¹ “Progress in adopting the principles for effective risk data aggregation and risk reporting,” January 2015, <http://www.bis.org/bcbs/publ/d308.pdf>.

² “Principles for effective risk data aggregation and risk reporting,” January 2013, Principle 1, 29(a), <http://www.bis.org/publ/bcbs239.pdf>.

³ Ibid.

⁴ Top Priorities for Internal Audit in Financial Services Organizations – Discussing the Key Financial Services Industry Results from the 2016 Internal Audit Capabilities and Needs Survey, <http://www.protiviti.com/en-US/Documents/White-Papers/Industries/Top-IA-Priorities-Financial-Services-Organizations-2016-Protiviti.pdf>.

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 Altamonte Springs, 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.

COPYRIGHT

Copyright © 2016 The Institute of Internal Auditors. For permission to reproduce, please contact The Center at FSAC@theiia.org.



Financial Services
AUDIT CENTER

Global Headquarters
The Institute of Internal Auditors
247 Maitland Avenue
Altamonte Springs, Florida 32701-4201, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org/FSAC