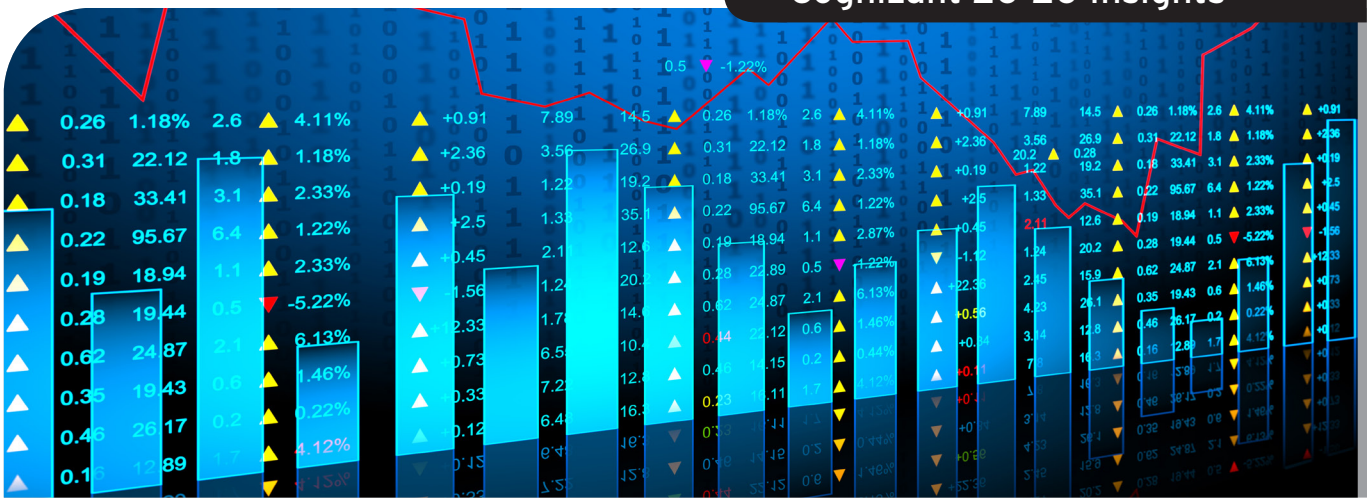
COGNIZANT



BCBS 239 Compliance: A Comprehensive Approach

When it comes to compliance, the BCBS 239 regulatory framework offers banks a lot of latitude. While global systemically important banks (GSIBs) have made progress in conforming to BCBS 239 principles, most domestic systematically important banks (DSIBs) remain in the early stages.

Executive Summary

In January 2013, the Basel Committee on Banking Supervision (BCBS) issued 14 principles for the effective aggregation of risk data and reporting. The intention was to address banks' ability to quickly and accurately understand and explain risk data and exposures, as well as the key risk metrics that influence their major decisions.

BCBS 239, which became effective in January 2016, applies to global systemically important banks (GSIBs).[1] Domestic systemically important banks (DSIBs) are expected to be compliant three years after being designated as such. The guiding principles of BCBS 239 for DSIBs are the same as those for GSIBs. While many GSIBs have made headway in complying with BCBS 239, most DSIBs are still in the early stages of the process.

BCBS 239 is not prescriptive; rather, it allows financial institutions to choose the approach that suits them best based on their business lines, risk profile and individual requirements. At the same time, BCBS 239's principles-based supervisory requirement[2] creates a degree of uncertainty regarding the appropriate approach for achieving compliance.

Compliance is also a challenge due to the large number of people, processes, data and infrastructure involved in managing risk for a major financial institution.

This paper presents a set of implementation techniques, along with recommendations and possible approaches, for complying with BCBS 239 principles.

Key Compliance Challenges

The typical issues facing financial institutions cross three dimensions: risk data aggregation, governance and infrastructure, and risk reporting (See Figure 1, next page).

Cognizant

BCBS 239 Compliance: The Challenges for DSIBs

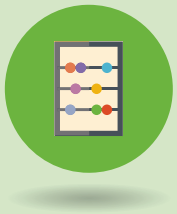
RISK DATA AGGREGATION	GOVERNANCE & INFRASTRUCTURE	RISK REPORTING
		
Risk Metrics • Risk metrics reported to the board and risk committees often cannot be traced – thereby failing to demonstrate data lineage. **Data Quality** • Data-quality issues with risk-data aggregators (such as the legal entity) and reliance on manual workarounds can have a significant impact on key risk numbers. • Inconsistent data terminologies, formats and structures, plus the lack of a single data inventory and dictionary add to the challenges of aggregating risk data.	**Governance** • Data management standards differ across banks' businesses. • Data architecture and taxonomy issues result in duplication and confusion. • Operational processes are not fully standardized across products and business units. **Technology & Infrastructure** • Differing views on optimal IT infrastructure (centralized and complex vs. decentralized and consistent). • Large technology and infrastructure projects are complex and drawn-out, and require significant investment.	**Impact of Risk Data on Reports** • Inconsistencies with reconciliation and data quality for reporting means risk reports will be inadequate. This points to the interdependency of data quality and risk reporting. **Controls, Checks and Process Deficiencies** • Controls, checks and balances and verification fall short. • Reliance on manual processes to create reports can invite errors.

Figure 1

Domestic systemically important banks face unique challenges due to their business mix and geographical location. Unlike GSIBs, they have not built out large technology infrastructures. Many rely on off-the-shelf products, rather than in-house development. Moreover, unlike GSIBs, they do not have the significant financial resources needed to pour into compliance initiatives. The type and nature of risk pillars differ between GSIBs and DSIBs. Most GSIBs have a greater presence in capital markets, and the type of risk exposures are more complex. DSIBs are more prevalent in retail and wholesale banking, and have limited exposure to capital markets and complex financial products compared to GSIBs.

Domestic systemically important banks face unique challenges due to their business mix and geographical location.

Most financial institutions are aware of BCBS 239 challenges but often fail to recognize interdependencies between BCBS principles.[3] For example, as part of their self-assessment, banks have rated themselves as largely compliant with risk-reporting practices, while acknowledging deficiencies in the areas of risk data aggregation, governance and controls.[4] However, gaps in risk data indicate that accurate risk reports cannot be generated.

Approaches for BCBS 239 Compliance

Every bank approaches BCBS 239 compliance differently. Some have begun documenting and cataloging their risk data. Others have started to analyze their risk-reporting processes and controls. Still others have attempted to streamline or overhaul the IT infrastructure supporting their risk and compliance functions.

There are three dimensions to BCBS 239 compliance: risk data aggregation, governance and infrastructure, and risk reporting.

Risk Data Aggregation

BCBS 239 requires that regulatory reports be based on risk data that is complete, accurate and clear at all times, including during crises, and presented to regulators and decision makers in time to allow for an appropriate response.

Since the data used for risk calculations is vast, it is important to concentrate on material data, rather than analyze all data elements. The first step is to identify the key lines of business and determine the material risk to the institution based on its current business profile. It is essential to focus on the risk data required for regulatory reports, key internal risk-management reports, as well as reports relevant to crisis management and stress testing.

Identify Material Risk Data

The main questions that banks should ask while identifying critical risk reports and material risk data are:

- What is the importance of a particular product or line of business to the financial institution, based on its business activities?
- What reports/data are used by the board or senior management to make critical business decisions?
- What reports/data are used by regulators, internal compliance and/or audit teams to determine the bank's risk profile?
- What reports are used during times of crisis or stress?
- What type of data is used to calculate or aggregate key risk metrics, such as risk capital and RWA?

Since the data used for risk calculations is vast, it is important to focus on material data.

The first task involves creating a consistent set of criteria for identifying material reports and data, and ensuring that the institution's senior risk-management committee approves the approach and the selected reports.

Institutions should also develop an inventory of enterprise-wide data management standards and processes, and specify critical elements of risk data, data transmission and data lineage. The next step is to confirm data gaps and identify their root causes. Banks can then create a plan for data standardization and remediation.

Perform a Pilot

Most financial institutions start with a pilot program for a particular focus area. As highlighted in Figure 2, the pilot can be based on a set of data attributes, an important repository, a set of reports or a specific product. Irrespective

Approaches for a Risk Data Pilot

Critical Data-Based

- Identify critical data elements across risk factors based on their use in decision making, materiality and regulatory reporting.
- Aggregate risk metrics by working with risk leadership within business units.

Repository-Based

- Identify key repository or risk-data warehouse within the organization.
- Confirm key data elements associated with the repository.

Report-Based

- Identify critical regulatory and internal management reports through discussions with senior risk executives.
- Obtain key data attributes associated with the report.

Product-Based

- Identify a specific product (Equities, FnO, Fixed Income, Loans, etc.) – preferably one that is material to the risk profile of the institution.
- Identify key data attributes associated with the product.

Figure 2

of the approach, it is important to select a broad spectrum of risk attributes. For example:

- **Credit exposure** is crucial, since it is aggregated across trades and business lines.
- **Legal entity** is significant, since it is used for risk aggregation.
- **Country of exposure** is important if the financial institution has a presence in multiple countries.
- **Trade date** is key due to its ubiquity.
- **Customer credit score** is more important for institutions that deal with credit cards and the retail segment.
- **Option sensitivities** are meaningful for derivatives market makers.

Execute a Firm-Wide Rollout

Once the execution method is finalized based on the pilot, the effort needs to extend across the institution to ensure it addresses critical risk data, key internal management and regulatory reports, and products. Figure 3 below details the phases of a firm-wide rollout.

Front-to-back data lineage is more onerous – requiring painstaking documentation and analysis. Data lineage can be performed manually, or by leveraging certain automation tools. Data gaps will generally emerge during the creation of glossaries, data dictionaries and data lineage documents.

BCBS 239 clearly states that in the event of non-compliance, banks must provide a remediation plan that is acceptable to supervisors.

As deficiencies increase in scale, regulators may propose additional supervisory requirements, including Pillar II capital measures. Therefore, the focus should be on putting controls in place or adopting temporary remedial measures for addressing the most critical weaknesses, while simultaneously creating a strategic roadmap for long-term solutions.

Governance & Infrastructure

Governance

In addition to their IT teams, banks' treasury, risk, finance and product teams must work together to align the governance of risk reporting frameworks and methodologies. There are some emerging practices followed by financial institutions to meet governance objectives for BCBS 239:

- The chief data officer (CDO) is accountable for data quality and data accuracy across the institution.

Executing a Firm-Wide Rollout

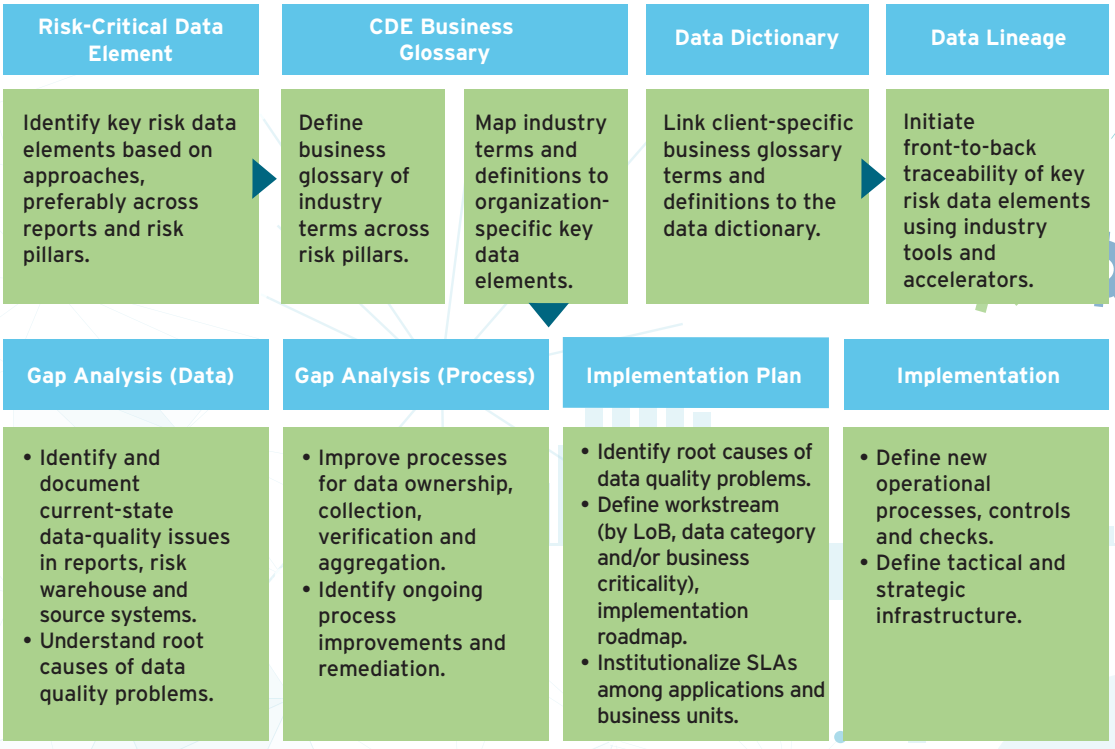


Figure 3

- Governance and coordination for all joint programs/projects (global PMO) across business units.
- Teams share responsibilities for risk, finance and treasury internal-management reporting, as well as external regulatory reporting.
- Processes are well defined, and process owners made accountable for results and decisions in all common/joint process areas.
- Data ownership is assigned and clearly defined.
- Integrated, centralized data taxonomies are established across the institution.

Infrastructure

Some financial institutions have considered overhauling their risk data repositories and reporting infrastructure in response to BCBS 239 regulations. Others have adopted a more tactical approach – concentrating on specific areas that include:

- Documentation & Service Level Agreements (SLAs)
  - Assure adequate documentation for risk infrastructure.
  - Integrate source systems and implement data-sourcing SLAs across platforms.
  - Formalize data exchange protocols across applications.
- Aggregation & Reconciliation
  - Update the risk aggregation rules engine.
  - Create metadata layers.
  - Build a reporting framework on top of the aggregation layer.
  - Build a reconciliation layer across source systems and the risk-data warehouse.
- Entitlements, Controls & Reporting
  - Set up a tools-based data certification process.
  - Implement ownership controls through centralized entitlements.
  - Assure ongoing health monitoring of technology platforms.

Risk Reporting

In self-assessment questionnaires from regulators, banks have consistently rated themselves high when it comes to risk reporting practices.

Some common activities associated with BCBS 239 compliance for internal and regulatory reports include:

- Identifying high-risk reports and report-generation process flows.
- Creating a reports inventory.
- Documenting data flows and reporting controls.
- Identifying report owners, consumers and control points.

Workflow reporting and process remediation can help spot control gaps in report flows and processes, and determine if controls are commensurate with the risk profile of reports and processes.

When a large number of process deficiencies are identified, they can usually be traced to manual errors in areas like data uploads, adjustments and checks. Ultimately, this leads to the creation of a remediation plan for process rationalization, standardization, and improving controls and checks around manual processes.

Our Point of View

Adopt a Customized Approach

Like any principles-based supervisory requirement, BCBS 239 can be interpreted in various ways and accommodate numerous implementation techniques. We have observed multiple compliance approaches – from focusing exclusively on risk data or reporting process remediation, to placing heavy emphasis on the technology infrastructure.

While all of these factors are essential, it is important to adopt a balanced approach that incorporates all aspects of BCBS 239 compliance; namely, risk data, regulatory and internal risk reports, processes, governance and technology infrastructure – all focused on meeting the regulatory objective of strengthening firms' risk-data aggregation capabilities and risk-reporting practices.

This requires financial institutions to identify their relative strengths and weaknesses on the BCBS 239 scale – leveraging the framework's "stocktaking" self-assessment questionnaire to customize a compliance approach.

Assess and Align Compliance Initiatves

Most financial institutions have concluded or are in various stages of compliance around data

governance and technology infrastructure. It is important to take stock of what has been achieved through these initiatives. In addition, programs for remediation need to be in sync with current projects to avoid duplications and redundancies..

Extract Business Value

In addition to remediation, financial institutions can realize operational benefits from the BCBS 239 compliance process. For example, BCBS 239 can be leveraged to streamline risk reports and processes, transform data, reduce risks and act as a driver for achieving firm-wide objectives for enterprise data management.

With the right approach and priorities in place, banks can meet certain compliance requirements around comprehensive data and reports for other regulations, including Comprehensive Capital Analysis and Review (CCAR) and Comprehensive Liquidity Assessment and Review (CLAR).

The advantages go beyond BCBS 239 compliance. Significant benefits can be achieved in areas like analytics, efficient capital management and reduced operating expenditures.

Given the significant costs associated with BCBS 239 compliance, DSIBs need to set priorities based on their business mix, identify common areas that will complement other programs, and focus on deriving true business benefits from the process.

Footnotes

[1] "Principles for effective risk data aggregation and risk reporting," Bank of International Settlements, January, 2013. http://www.bis.org/publ/bcbs239.pdf.

[2] Ibid.

[3] "Progress in adopting the principles for effective risk data aggregation and risk reporting," Bank of International Settlements, January, 2015. http://www.bis.org/bcbs/publ/d308.pdf.

[4] Ibid.

About the Authors

Mrugesh Kulkarni is a Principal in the Capital Markets and Risk Practice for Cognizant Business Consulting in North America. He has conducted many large organizational and regulatory implementation projects for risk and compliance in the U.S. Recently, he has focused on BCBS 239 implementations, OTC derivative clearing, Fundamental Review of Trading Book (FRTB), and Basel III-related engagements. He holds an MBA from the Indian Institute of Management, Lucknow, and a bachelor's degree in engineering from Mumbai University. Mrugesh is a member of the Global Association of Risk Professionals, and has completed the FRM certification. He can be reached at Mrugesh.Kulkarni@cognizant.com | https://www.linkedin.com/in/mrugesh-kulkarni-6253344.

Sudhir Gupta is Vice President and co-leader of Cognizant's Capital Markets and Risk and Compliance Consulting practices in North America, with a team of over 200 consultants dedicated to improving companies' business processes and IT portfolios. He has worked with asset managers, asset servicers, custodians, institutional broker dealers, and retail and prime brokers to drive business model innovation, operational excellence, business and IT strategy planning, and business case development. He can be reached at Sudhir.Gupta@cognizant.com | https://www.linkedin.com/in/sudhir-gupta-1336922.

About Cognizant Business Consulting

With over 5,500 consultants worldwide, Cognizant Business Consulting offers high-value digital business and IT consulting services that improve business performance and operational productivity while lowering operational costs. Clients leverage our deep industry experience, strategy and transformation capabilities, and analytical insights to help improve productivity, drive business transformation and increase shareholder value across the enterprise. To learn more, please visit www.cognizant.com/consulting or email us at inquiry@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 100 development and delivery centers worldwide and approximately 233,000 employees as of March 31, 2016, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
1 Kingdom Street
Paddington Central
London W2 6BD
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com

© **Copyright 2016, Cognizant.** All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.

Codex 1888