WHITE PAPER

Decoding BCBS 239 compliance for optimal risk management

Infosys®

Introduction

After the 2007–08 financial crisis, banks realized that they had failed to manage their operational risks due to poor and ineffective risk data aggregation capabilities and an inefficient risk data reporting architecture, which resulted in losses worth billions of dollars. Typically, different lines of business (LOBs) of the bank worked in silos, which made it difficult to present one consolidated picture of the risk level it was dealing with. Some banks were even completely missing an enterprise risk management (ERM) framework, needed to consolidate data and make quick decisions.

As a response to the 2007–08 financial crisis, the Basel Committee on Banking Supervision (BCBS) came up with 14 guidelines or principles that are being considered as supplemental to Pillar 2 (supervisory review) of Basel II. Collectively, these principles would be called BCBS 239 and issued to enhance a bank's capabilities in aggregating and reporting risk data efficiently. The 14 principles can be categorized in four segments illustrated in the exhibit alongside.

Exhibit 1: The four categories of BCBS 239 principles

Let's begin by understanding each category.

Governance and infrastructure

This category focuses on the governance models that banks employ to monitor / frame policies on their risk mitigation / transfer capabilities. It also includes the roles and responsibilities that the top management is expected to play in risk data management (aggregating / processing / reporting). Documentation is an integral part of this principle and involves listing the risk framework, risk appetite, risk tolerance statements, and the principles validated and verified by the board of directors. From an infrastructure perspective, this category covers the existing IT infrastructure of banks and evaluates their capability to support strong risk data aggregation and efficient reporting.

Risk data aggregation capabilities

This category covers various attributes such as accuracy, completeness, integrity, and adaptability with which the risk data should be enriched before reporting. Before the data is reported to the board of directors (BOD), it is crucial to ensure that all aspects of risks have been considered and collected (including off-balance-sheet items). It is also important to send up-to-date reports in a timely manner, without compromising on the accuracy, integrity, or completeness of the data they hold.

Risk reporting practices

This takes into consideration the accuracy, comprehensiveness, clarity, and usefulness of the reports that are sent for review to the regulatory agencies. It is paramount that the reports have the required levels of granularity for the regulatory bodies to assess the risk levels of the bank. The category also considers the frequency at which the reports are sent. Banks have to send the reports at regular intervals, without missing service level agreements (SLAs) / deadlines.

Supervisory review, tools, and cooperation

This category details the supervisory review to evaluate a bank's status on being compliant with other regulations. Supervisors should also monitor the remedial actions taken by banks to ensure compliance with the principles. The category also monitors the meeting of supervisors from different jurisdictions to discuss the principles' implementation status.

External Document © 2016 Infosys Limited

How implementing these principles can help a bank?

Many banks have already realized the benefits of implementing the BCBS 239 principles. On the one hand, the principles have proved to be a tool to enhance risk data aggregation and reporting capabilities, while on the other, it has helped them in strategic planning.

Four key advantages of adopting these principles are:

The golden picture

The aggregated data presents a consolidated picture of the risk data from across the enterprise. Connecting these data sets provides a holistic view to the top management of the risks that the bank's assets / entities are exposed to.

Minimal losses

A unified, single-page picture of risk data provides banks an opportunity to take actions pre-crisis, rather than performing a post-crisis analysis. This can effectively reduce the severity and the chances of losses that banks may incur due to poor data visibility caused by taking a 'siloed or isolated' approach. Banks can also save on efforts required to access data.

Strategic planning

Risk data aggregation enhances the decision-making capability of banks. It enables the top management to see the magnitude and likelihood of risk and helps manage the risk-return trade-off for the bank. This makes it easier to decide if a strategy or business plan should be implemented. It also helps identify the core vs. non-core risks for a business, which in turn, enables banks to decide what is better – transferring, ignoring, or taking the risk to take better advantage of available opportunities.

Risk-bearing capacity

By looking at the aggregated picture of the various risks present across the bank, the top management can decide how much risk the bank can take without losing the confidence of its stakeholders and customers. Visibility into an organization's risk-bearing capacity helps the management decide if a new project, product, or service will have any potential impact on the bank's financial stability.

External Document © 2016 Infosys Limited

Implementation challenges

Even today, implementing these principles is not easy. Banks face an array of challenges while aggregating data pertaining to all the material risks from across their LOBs. Reporting too, is a significant challenge. Here's a list of some of the challenges:

No numbers, only principles

Regulators have put in place these principles in an effort to make it easier for banks to comply with regulations. However, there are no numbers that the banks need to report. Due to this qualitative approach taken by regulators, banks are unsure whether the measures taken are adequate to provide an acceptable picture to the regulators.

LOBs working in silos

Given the differences in the data architecture and reporting framework of each LOB in the bank, each unit works in its own silo to report risk data to the top management. With BCBS 239, there is now a need to consolidate this data, which has given rise to a significant challenge – aggregating all the data and creating a repository, even though it comes from different sources and in different formats. To make matters worse, in some cases, the units are not synchronized in terms of the data they report.

Capital involved in scaling up

Banks currently lack the IT infrastructure and architecture required to aggregate all the risk data. To re-engineer the existing architecture and replace the legacy IT infrastructure, banks need to invest huge capital on additional manpower, hardware, and solutions. The extra capital could potentially cause issues with their budget planning and could also affect strategic planning.

No defined metrics to measure

One of the biggest challenges currently faced by banks in being compliant with the principles, is the absence of any tools or metrics to measure their compliance levels. Banks not only have to define the metrics, but also the acceptable threshold levels. Even if the aggregation and reporting capabilities related to risk data are scaled up, without the presence of tangible metrics, it will only be half the battle won.

External Document © 2016 Infosys Limited

The time window that is worrying banks

The Basel Committee set January 2016 as the deadline by which banks declared as Global Systemically Important Banks (G-SIBs) by the Financial Stability Board (FSB) had to comply with the principles. The committee also specified a timeframe of three years for non-G-SIB banks to comply with these principles.

According to a report published by the Basel Committee on the progress made till 2014, 14 G-SIBs would not be compliant with 11 of the 14 principles. There would be at least one principle because of which the status of these G-SIBs would be red (non-compliant). Reports also suggest that it would take another two years (2016–2018) for the banks to be fully compliant.

Banks designated as Domestic Systemically Important Banks (D-SIBs) by their respective countries have also shown similar results (not being fully compliant).

Recommended solution

Outlined below are five steps that would help banks achieve compliance with the principles:

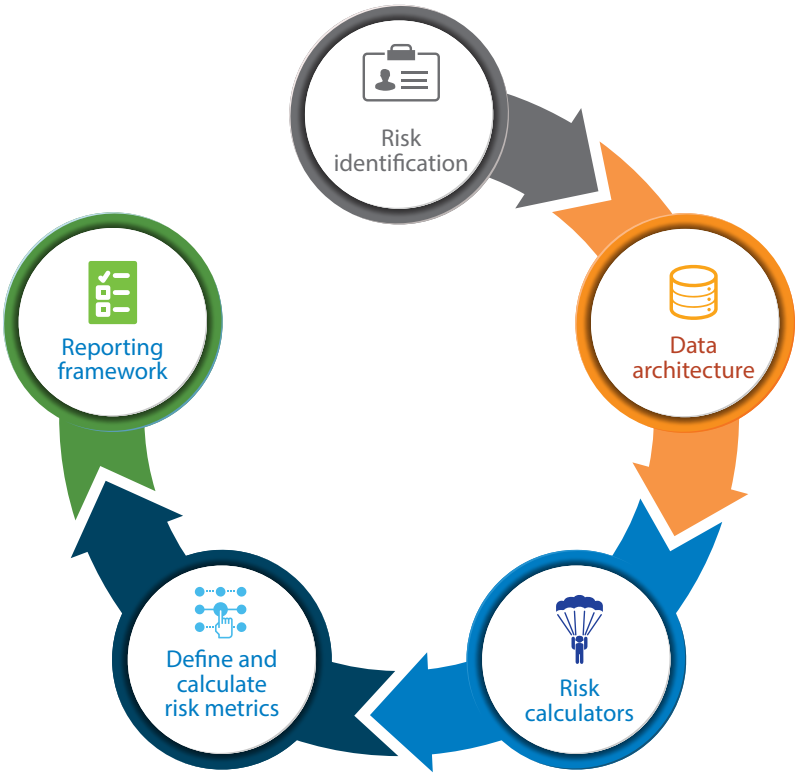

Exhibit 2: Steps to be compliant with BCBS 239 principles

- **Risk identification**
  This is the first and foremost step. Banks need to carry out a detailed study of their existing systems to assess the feasibility of integrating different systems. Once the risk is identified, the top management can decide which risk to take and which ones to pass.
- **Creation of data hub**
  This step involves defining the repository / hub where risk data can be parked. Data from different sources will be put into the hub after an initial cleansing and transformation process. The hub can be a 'data lake' or an integrated risk data warehouse.
- **Calculation of risk data**
  The repository will serve as a hub from where the various risk engines will pick the relevant data for calculating metrics. Once the calculations are done, the data is again put into the repository so that the entire reporting can be done from one central point.

External Document © 2016 Infosys Limited

- ## Definition and calculation of risk metrics for BCBS 239

  Banks need to define tangible metrics that can validate data so as to check if the data in the repository adheres to the principles (defined above) for BCBS 239. The detailed process of defining and calculating metrics is mentioned below:

Table 1: List of metrics to be calculated for the 14 principles

Principle	Category	Description	Metrics considerations
1	Governance and infrastructure	Governance	• Process for aggregation and reporting of risk data • Documentation of processes followed for aggregation and reporting • Roles and responsibilities of the top management in data management
2		Data architecture and IT infrastructure	• Backup and restore mechanism • Masking / encryption of sensitive data when it is processed / moved from one layer to another
3	Risk data aggregation capabilities	Accuracy and integrity	• Accurate metadata for all the data elements • A common platform where the data from different sources can be collated in one format • Frequency of checking data for accuracy and integrity
4		Completeness	• Ensuring that relevant data sources are sending data to the common repository • Reconciliation processes and their stages • Percentage of mandatory fields that are filled in various forms such as the Know Your Customer (KYC)
5		Timeliness	• SLAs for meeting data requirements not just under normal, but also in stress conditions • SLAs for meeting regulatory norms
6		Adaptability	• Customizability of data for user's need
7	Risk reporting practices	Reporting accuracy	• Process for reconciliation and validation of reports • Definition of acceptable variance while reconciling data • Clear reporting process to resolve and mitigate errors
8		Comprehensiveness	• Sufficient data to report all kinds of risks • Drill down capabilities in report to cover the risk at the most granular level
9		Clarity and usefulness	• Usefulness of reports for decision making • Interpretation and the intention of reports should be the same across teams
10		Reporting frequency	• Frequency at which the reporting is done • Capability to change this frequency as per user's requirement
11		Reporting distribution	• Classification of reports as confidential, public, and internal, before distribution • SLAs for the distribution of reports to the concerned team • Approvals for the creation / update / removal of distribution list
12	Supervisory review, tools, and cooperation	Review	• Levels of review to be made • Logging of review comments – manual / tools • Incorporation of review comments
13		Remedial actions and supervisory measures	• Remedies for overcoming shortages to achieve required capabilities for aggregation and reporting of risk data • Supervisory body in banking entity to keep internal checks • Scope / functions of the internal auditors
14		Home or host cooperation	• Timely compliance with regulations • Timely responses to concerns raised by regulators regarding reporting by the banking entity

- ## Reporting framework

  Once the metrics are calculated and stored in the data repository, they are reported to the top management and various regulatory bodies as per the defined SLAs.

External Document © 2016 Infosys Limited

Conclusion

During the post analysis of the financial crisis of 2007–08, BCBS realized the importance of having effective and efficient risk data aggregation and reporting capabilities in place for a financial institution and came up with some guidelines. These guidelines were eventually named as the 14 principles of BCBS 239. The committee also realized that with the current infrastructure, banks would need some time to adhere to the principles. Hence, the banks were allowed the flexibility to implement the principles in an incremental mode.

Banks are still struggling to comply with the 14 principles prescribed by the Basel Committee. They are still in the process of leveraging their existing infrastructure to efficiently manage their capabilities for risk data aggregation and reporting. It is recommended that such banks take note of the metrics provided in this whitepaper.

References

http://www.bis.org/bcbs/publ/d348.pdf

http://www.bis.org/bcbs/publ/d348.htm

https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-15-2733H-risk-data-aggregation-reporting-BCBS-239.PDF

http://www.ey.com/Publication/vwLUAssets/EY-bcbs-239-risk-data-aggregation-reporting-AU/$FILE/EY-bcbs-239-risk-data-aggregation-reporting-AU.pdf

https://blog.knowledgent.com/14-principles-bcbs-239/

External Document © 2016 Infosys Limited

For more information, contact askus@infosys.com

© 2016 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names, and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording, or otherwise, without the prior permission of Infosys Limited and/or any named intellectual property rights holders under this document.

Stay Connected