The concrete impacts of BCBS principles on data value chains

Jean-Pierre Maissin
Partner
Technology & Enterprise Application
Deloitte

Jean-Philippe Peters
Partner
Governance, Risk & Compliance
Deloitte
The application of the BCBS 239 regulation will have a direct consequence on banks’ data management. Indeed, all of the principles exposed in the text aim to push banks towards risk evaluations based on optimized, documented and transparent data usage. Banks have to deal with several challenges that can be tackled without too much difficulty if they perform the right technological component selections and organizational designs.

Context
In January 2013, the Basel Committee on Banking Supervision published the BCBS 239 paper: “Principles for effective risk data aggregation and risk reporting”. The objective of this regulatory framework is to ensure that data used for risk calculation and, ultimately, the required capital definition, is of the appropriate level of quality. Furthermore, over time it will enable the decision-making process to be improved, and losses due to bad risk management to be reduced within all relevant banking institutions. This means that not complying with these principles would jeopardize the trust of regulators in the provisions made by banks, which could lead to capital add-on.

At this stage, G-SIBs and D-SIBs are affected by this regulation but within different timeframes (1 January for G-SIBs, three years after designation for D-SIBs). This way, G-SIBs and D-SIBs are at different stages of implementation but SIBs will have to prioritize and efficiently organize their project portfolios to meet deadlines.

The BCBS 239 principles represent an opportunity to improve data management and IT infrastructure. Making appropriate investment in information systems will generate enterprise-wide benefits, such as data quality, process optimization, and improvement of decision-making processes.
What are the requirements of BCBS 239?

How BCBS 239 requirements impact the data value chain

A typical data value chain can be seen as the succession of four main steps:

1. Data collection, which enables all the required information used to calculate risks to be centralized. There can be different types of sources, as they are associated with specific applications from each banking department.
2. Data quality controls must then assess the reliability of data and demonstrate that the level of quality is sufficiently high for risk assessment purposes.
3. Data aggregation can take place once the data has been collected, cleansed and validated by its owners. This step is particularly sensitive as it must be flexible enough to quickly accommodate market changes and potential new risk drivers.
4. Finally, reporting shall be produced. This step must take into account strict constraints, such as enabling banks to answer ad hoc inquiries from the management or the regulator very quickly in stress situations.

The following diagram presents a representative extract of BCBS 239 principles that can be mapped as requirements on the different steps of a typical data value chain:

Data quality controls must assess the reliability of data and demonstrate that the level of quality is sufficiently high for risk assessment purposes.
Banks should develop and maintain strong risk data aggregation capabilities to ensure that risk management reports reflect the risks in a reliable way.
The data governance aspects should not be underestimated as this may have significant impact on the bank’s organization.

This mapping enlightens four major areas of impacts to consider to meet the requirements:

1. **Data quality technology**
   The technology components for data quality controls should be robust but flexible enough to meet the accuracy and adaptability principles.

2. **Reporting technology**
   The reporting technology should encompass strong visualization, exploration and self service capabilities to meet clarity and adaptability principles.

3. **IT Governance**
   The impact on IT governance and especially release management may be significant as the BCBS will require more agility in the release cycle to reduce the time to provide the end users with new reporting.

4. **Data governance**
   Although most of banks already took this into account, the data governance aspects should not be underestimated as this may have significant impact on the bank’s organization.

**How can banks meet these requirements?**

As we have seen, aside of the data itself, banks will have to act on the governance, process and technology side to comply with the BCBS239 requirements.

**Data quality technology**

The architectural choices to be performed when implementing the data quality technology shall be weighted carefully as they might imply significant recurring costs. In the context of Solvency II, many insurers realized that a standardized approach, although requiring more investment at implementation, has an excellent return on investment considering the significant number of controls to be performed. Concretely, this standardized approach is based on a standard set of controls that are parametrized to meet the specificities of the different data sets. In other words, instead of implementing new rules for each dataset, the project team only defines a small set of parameters. This approach drastically reduces implementation costs as well as recurring costs. Furthermore, it enables a much more systematic approach towards quality control.

While many of-the-shelf packages covering these functionalities exist on the market, it is very unlikely that banks will find the solutions that fits into their (often complex and heterogeneous) IT landscape. It is therefore expected that like insurers in the context of Solvency II, many actors will deploy their own data quality IT component to get the best balance between cost, integration and effectiveness. Depending on the existing data architecture, this new component will typically occur at the entrance of the data lake, data warehouse or risk data mart.
Reporting technology
Although many organizations have reporting and visualization tools used within different departments, only few of them govern these tools centrally and are able to assess if they can meet the BCBS requirements. The first challenge will therefore be to get a common understanding of the as-is situation to identify if there is a need to select a new reporting tool or not.
On the tool selection itself, we have analyzed the market of reporting and analytics IT packages and noticed that a lot of solutions exist, but, unfortunately, it is impossible to find any ‘one size fits all’ solution. To meet both adaptability and accuracy principles, banks will have to evaluate their own reporting landscape and often consider the addition of new reporting components. Considering the timelines, the analysis and the tool acquisition processes to conduct, these activities should be started as soon as possible.

IT Governance
To meet flexibility requirements, a two-speed development model may be put in place. Today, most organizations follow release calendars, preventing them from reaching the forthcoming flexibility constraints. In order to tackle this challenge, IT organizations will consider that some components will have to be moved to a faster release cycle management process.

Data governance
To meet BCBS expectations, organizations will have to be increasingly data driven. Strict data governance is needed to support the end-to-end data flows, and has to be organized with every business unit in the bank. This means that ownership and stewardship of the data has to be clearly defined, agreed and known in the organization, as well as the data management processes.

How far along are the banks today?
The Basel Committee has published a progress report entitled ‘Progress in adopting the principles for effective risk data aggregation and risk reporting’ (BCBS 268). This is based on a self-assessment survey completed by the largest banks and supervisors. In particular, the report underlines that “many banks are facing difficulties in establishing strong data aggregation governance, architecture and processes”, and are resorting to “extensive manual workarounds”. Banks need to “significantly upgrade their risk IT systems and governance arrangements” to address these shortcomings.

Conclusion
The application of the BCBS 239 regulation will have direct and significant consequences for banks’ data management. To meet these challenges, banks will have to consider the adoption of generic components to manage data quality and also conduct an appropriate review of their reporting tool. On top of this, successful implementation will not happen without new approaches to data governance and release management. These major changes shall be addressed with a broader perspective with for example an enterprise data warehouse in order to get benefits for the whole company in terms of reporting and make a viable business case out of the regulatory constraints.