BCBS 239
Zoom on the scope

Jean-Pierre Maissin
Partner
Technology & Enterprise Application
Deloitte Luxembourg

Loic Saint Ghislain
Senior Manager
Technology & Enterprise Application
Deloitte Luxembourg

Context

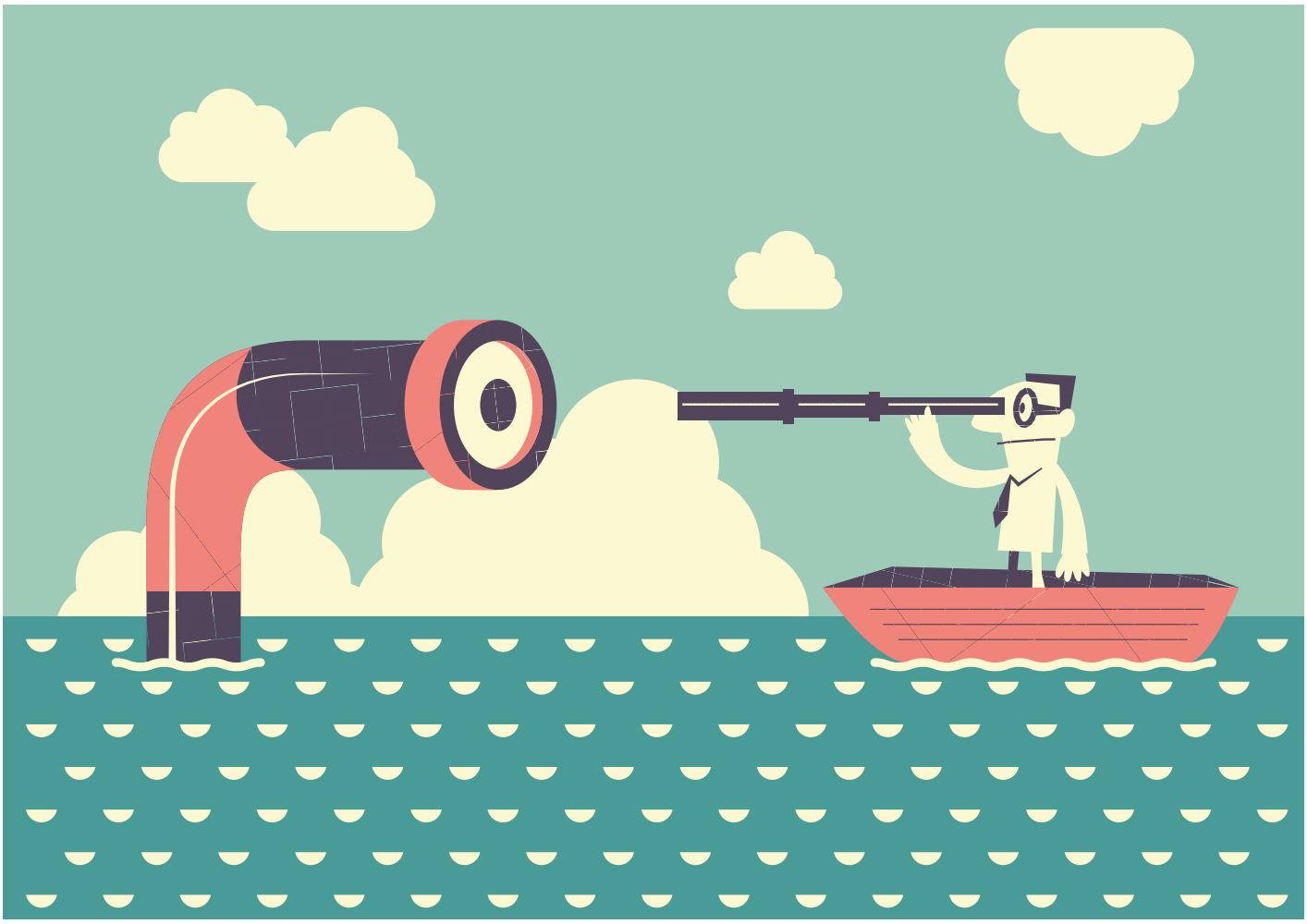
In January 2013, the Basel Committee on Banking Supervision published the BCBS 239 paper: "Principles for effective risk data aggregation and risk reporting." Impacts of the publication are significant for "global systemically important banks" (G-SIBs) and "domestic systematically important banks" (D-SIBs) as it defines strong requirements in terms of data management. The objective of this regulation is to ensure that data used for risk calculation and reporting have the appropriate level of quality and that the published risk figures can be trusted. This implies that not complying with these principles would jeopardize the trust of regulators, which could lead to capital add-on. At this stage, both G-SIBs and D-SIBs have been identified. The lists are available from ECB or CSSF as per the Regulation 15-06.

On the other hand, BCBS 239 is a data-intensive regulation with strong data quality requirements, implying that data quality management should addressed cautiously, not only on risk data, but throughout the bank. Indeed, data quality issues have already been the cause of significant losses through a lack of productivity or incorrect decision making. A significant example of poor data quality impact is an online banking provider that lost many customers who opted-out of receiving future solicitations from their provider because they repeatedly sent offers for products they already owned.

The application of the BCBS 239 regulation will have a direct consequence on the data management of banks. Indeed, all of the principles explained in the text aim to push banks toward 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.

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 the improvement of the decision-making process.

The application of the BCBS 239 regulation will have a direct consequence on the data management of banks.



Three categories of principles and requirements

I. Overarching governance and infrastructure

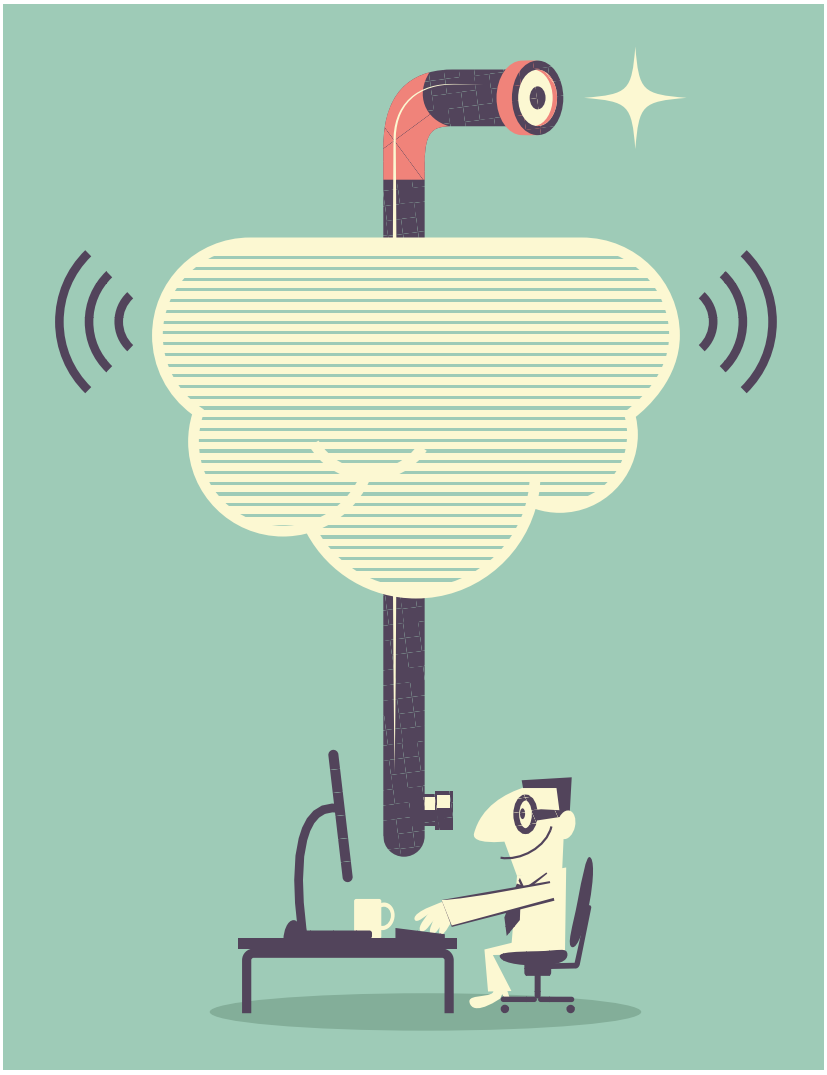
These principles mainly cover two fundamental aspects of data management: sponsorship and IT infrastructure.
The point here is to ensure ownership of the risk data aggregation processes by senior management in order to put an appropriate level of controls in place. This also requires the IT infrastructure to be robust and resilient enough to support risk reporting practices at a time of stress and crisis. For example, risk reporting should be integrated into the BCP of the bank, and a bank should establish integrated data taxonomies and architecture across the banking group.

II. Risk data aggregation capabilities

The main focus of these principles is the processes and controls put in place prior to risk calculation. It especially focuses on data quality monitoring, the procedures applied, and the documentation produced (e.g., definition of the single point of truth for all data or maintenance of a cross functions data dictionary of terms). It considers most of the dimensions of data quality from accuracy to timeliness. It also recommends adaptability of the processes to enable fast decision making.

III. Risk reporting practices

With these principles, data quality is again emphasized in this category with reference to the accuracy of the reporting made. It also recommends clarity in this reporting to make it useful for senior management in decision making. For example, it is necessary to define requirements and processes to reconcile reports to risk data or that the frequency of reports should be increased during times of stress or crisis: "Some position/exposure information may be needed immediately (intraday) to allow for timely and effective reactions."



The concrete impacts of BCBS expected

How will BCBS 239 requirements affect operations and business?

Impacts for CROs

Not surprisingly, the Risk Management team will be highly affected by the new principles. If we take for example the concentration risk modelling, the principal role of the Risk Management team today is to build a model that appropriately measures the concentration risk for the organization. Obviously, any model requires input data and this is where the BCBS 239 principles apply: in order to ensure completeness, accuracy, and integrity, it is necessary to clearly define the data requests that are to be handled by the back office departments. These definitions, as required per the model, will have to be formalized and documented by the Risk Management team. On top of this, the Risk Management team will have to be ready to answer ad hoc requests from the regulators. Obviously, they will rely on IT departments to support them in getting the data and implementing automations, but they will be responsible for the effectiveness of the control of the data quality in the end. This means that the Risk Management team will have to play a significant role in the governance of the risk data. Risk Management will also be affected as it must be able to face these new challenges with the appropriate skills, e.g., project management, requirements analysis, and formalization—skills that were not strictly needed before.

However, the Risk Management team is not the only team affected by the principles; other entities in organizations should also prepare for change.

Impacts for COOs

Back office teams will also be affected, as they are the main data providers of Risk Management. This means that they have to be proactively involved in the data governance and the data quality process in order to be able to anticipate data requirements or corrections to be performed—to have the capacity to deliver accurate data in a timely manner. Data requirements may lead to identification of gaps, as for detailed collateral data in the AQR exercise. Filling these gaps may induce significant workload in the back office teams to record this missing data in an electronic format. This will also mean a probable impact on the underlying systems and tools that will require updates or new developments, which will affect the overall capacity of the teams as per their involvements in implementation projects. The COO will then face the choice of determining the level of functional coverages and related investments in the IT tools depending on the target remaining operational workload on the long run. Finally, the back office functions could be in a position of shared ownership for specific

data. For example, client-related data might be cross-functional in the organization, which requires alignment from all departments to have unique, agreed, and validated data structure and content of this data.

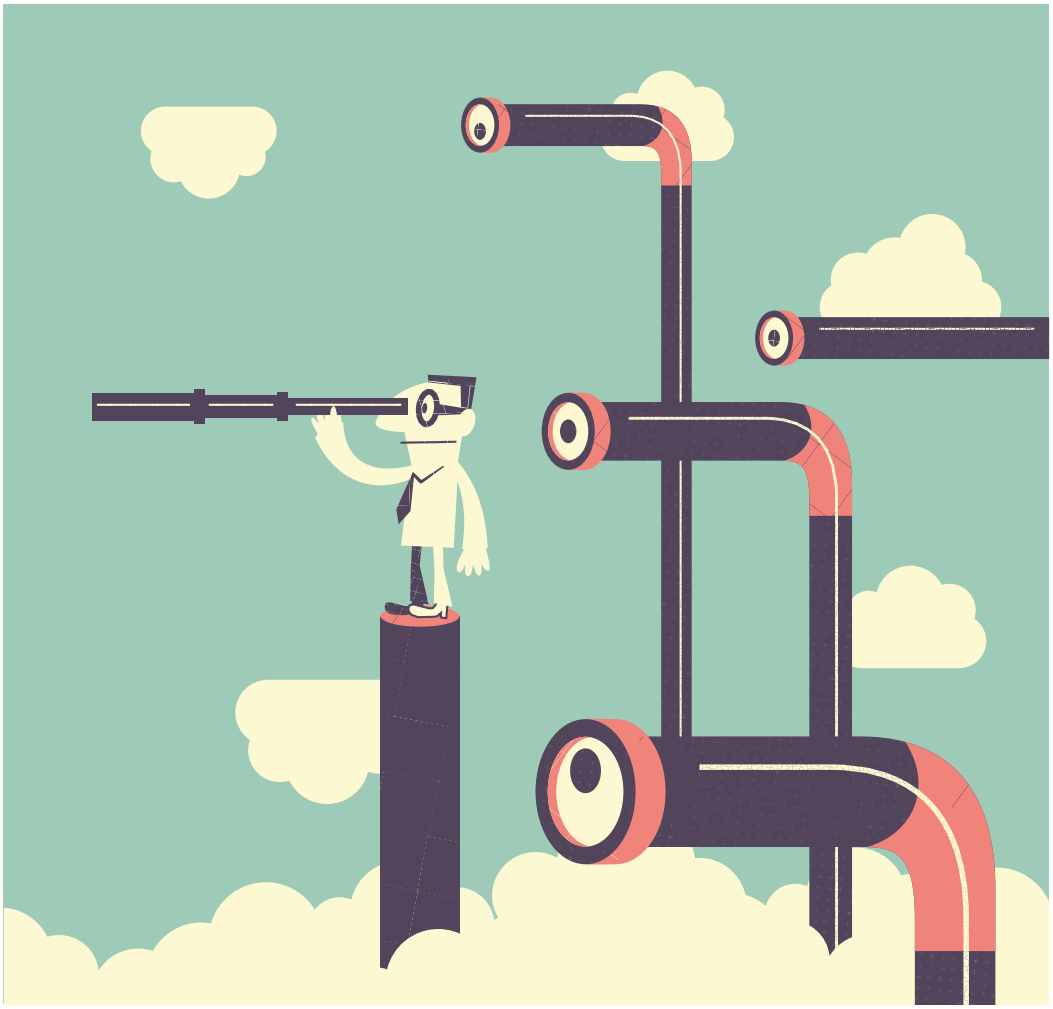
Impacts for HR management

The impacts described above will lead organizations to look for different skillsets than the usual ones. Looking at the insurance sector and how Solvency II has affected it, we can clearly anticipate that banks will in turn look for new business profiles that have experience in IT development projects, good knowledge of algorithms and automation, SQL, and data modelling. These types of profiles will leverage on technical and data skills to enhance organizations' efficiencies in the design of their risk models and reports. This means that HR functions will have to be able to detect and assess this new variety of skills and competencies to include these in their recruitment plans.

Impacts for CIOs

Information technology departments will certainly be affected in the support that they will provide to Operational and Risk teams. On top of this, they are likely to be leaders in the technical and functional gap analysis to be performed on existing reporting chains (Basel III for example) to identify gaps and propose resolutions to meet BCBS239 requirements. Below is an example on how BCBS 239 can have an impact on a typical data value chain, which will have to be managed and maintained within the CIO's responsibilities.

The Risk Management team will have to play a significant role in the governance of the risk data.



How will BCBS 239 requirements affect the data value chain?

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 strict constraints into account, such as enabling banks to answer ad hoc inquiries from the management or the regulator very quickly in stressful situations.

The different steps of a typical data value chain highlight four major areas of impacts to consider:

Data governance
Although most banks have already taken this into account, data governance aspects should not be underestimated, as this may have significant impact on the bank's organization.

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.

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

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

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. These generic components should be designed or bought thinking about other regulatory challenges involving data such as GDPR or MIFID regulations in order to maximize the reusability of the tools.

Targeting compliance should not prevent banks from making the few steps further to high business value impact. Indeed the adoption of a data management framework can help banks to efficiently leverage from regulatory obligations to operational gains.

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 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.

Along with this, the changing IT infrastructure and applications landscape should lead to further reflections in the use of new technologies such as digital channel enablers or data lakes, which will be decisive for leading banks to stay ahead of the pack in the future.