BCBS 239 Operational impacts

Jean-Pierre Maissin
Partner
Technology & Enterprise Application
Deloitte

Martin Flaunet
Partner
Banking Leader
Audit - Banking & PSF
Deloitte

Ronan Vander Elst
Director
Technology & Enterprise Application
Deloitte

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 implementation of such principles are significant for *"Global Systemically Important Banks"* (G-SIBs) as it defines strong requirements in terms of data management. The main objective of this reform 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 jeopardise the trust of the regulators which could lead to capital add-on. At this stage, only G-SIBs are concerned but regulators strongly recommend to apply the same rules for Domestic Systemically Important Banks (D-SIBs), which may lead to wider scope of regulation. The timeline for expected implementation for G-SIBs is the beginning of 2016.

The requirements are based on 14 principles, organised in four categories, the fourth one being for the local regulators

Principles for effective risk data aggregation and risk reporting

01/

Overarching governance and infrastructure

1. Governance

- Governance rules for aggregation of risk data and risk reporting
- Data (quality) management as a responsibility of top management
- Clear roles and responsibilities on data and data quality for staff with IT, business and reporting expertise

2. Data architecture and IT infrastructure

- Extension and maintenance of documentation on internal data and IT- architecture
- Comprehensive support for aggregation of risk data and risk reports
- Capability of infrastructure to support risk data aggregation and reporting practices during times of stress and crisis

02/

Risk data aggregation capabilities

3. Accuracy and integrity

- Accurate and reliable risk data in normal and stress situations
- Largely automated aggregation for minimising the probability of errors
- Data (quality) management incl. data controls as robust as those applicable to accounting data

4. Completeness

- Gathering/aggregation of all relevant risk data over all group units
- Diverse reporting dimensions at group level (legal entity, business unit, asset class, industry etc.)
- Availability and flexibility of required and utilised reporting dimensions

5. Timeliness

- Generation and provisioning of risk data depending of criticality and volatility as well as based on the characteristic and overall risk profile of the bank
- Bank/business specific reporting frequency
- Generation of risk data while also meeting the principles relating to accuracy, integrity, completeness and adaptability

6. Adaptability

- Ability to respond to ad-hoc risk management reporting requests
- Adaptability in case of new assessment requirements during crisis/stress situations
- Flexible and efficient analysis architecture
- Simulation/forecast of risk information

03/ Risk reporting practices

7. Accuracy

- Accurate and correct consolidation of aggregated reporting data
- Processes to reconcile reports to risk data
- Data(quality) management
- Expectation of high reporting quality as the basis for critical and strategic business decisions

8. Comprehensiveness

- Coverage for all material risks
- Depth and scope of reports reflecting the type and complexity of businesses and bank's risk profile
- Reporting cover based on the requirements of recipients
- Forward-looking assessment of risks

9. Clarity and usefulness

- Clear and concise manner of reports for facilitating informed decision making
- Appropriate balance between risk data, analysis and interpretation as well as qualitative explanations
- Demonstration of the usability of reports for management decision making

10. Frequency

- Determination of reporting frequency based on recipient, risk and purpose
- Dependency on type and volatility of risks, the relevance to risk management and efficiency of decision making
- Increase in frequency in case of stress/crisis situations

11. Distribution

- To relevant parties
- Security on confidential material
- Relevant reporting procedures and access rights

04/ Supervisory review, tools and co-operation

12. Review

- Regular control and evaluation of compliance with the eleven principles of BCBS 239
- Test of conformity and reaction times on compilation of risk data and reports

13. Supervisory measures

- Introduction of measures to remove any deficits and shortages in achieving relevant capabilities for aggregation of risk data and risk reporting
- Allocation of target timeline by relevant regulator body for implementation
- Use of instruments for reducing risks under Pillar 2 (e.g. introduction and use of specific risk and acquisition limits)

14. Home/host cooperation

- Co-operation with relevant regulatory bodies for assessing the compliance with the requirements and by execution of relevant measures to remove any identified deficits regarding the principles

Expected operational impacts

Impact on CROs

Not surprisingly, Risk Management teams will be highly impacted by the new principles. If we take for example the concentration risk modelling, the principal role of Risk Management teams today is to build a model that measures appropriately the concentration risk for the organisation. Obviously, any model requires input data, and this is where BCBS 239 principles apply: ensuring completeness, accuracy and integrity will require clearly defining the data requests that are to be handled by the back office departments.

These definitions, as required per the model, will have to be formalised and documented by Risk Management teams. In addition to this, Risk Management teams will have to be ready to answer ad hoc requests from 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 Risk Management teams will have to play a significant role in the Governance of the risk data. Risk Management will also be impacted as it must be able to face these new challenges with the appropriate skills, such as project management, requirements analysis and formalisation—skills that were not strictly needed before.

However, Risk Management will not be the only one impacted by the principles, other areas/departments in the organisation should also prepare for change.

Impact on COOs

Back office teams will also be impacted because they are the main data providers of the 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. Moreover, they need 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 recent 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 probably have an impact on the underlying systems and tools that will require updates or new developments, which will impact the overall capacity of the teams as per their involvement in implementation projects. The COO will then face the choice of the automation level of the data management activities, depending on the target operational workload in the long run.

Finally, the back office function could be in a position of shared ownership for specific data. For example, client related data might be cross-functional in the organisation, and would require alignments from all departments to achieve unique, agreed and validated data structure and content.

Impact on CIO

Information technology departments will certainly be impacted in the support they provide to Operational and Risk teams. In addition to 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 resolution plans to meet the BCBS 239 requirements.

Impact on HR management

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

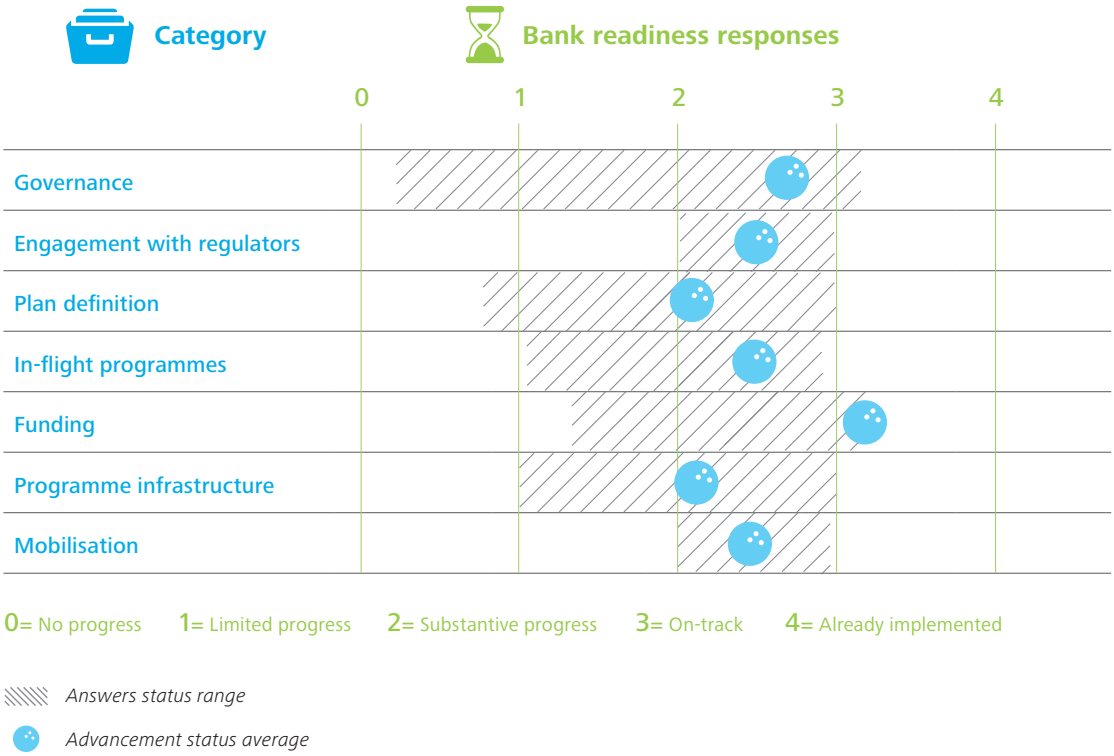
Market readiness

Every six months since December 2013, Deloitte has been conducting a survey on market readiness toward BCBS 239 among SIB's (note that for Luxembourg the list has not been disclosed at this stage). It focuses on two aspects of BCBS 239 for Banks: advancement of implementation project and compliance readiness. Results and trends presented hereunder reflect the declarations of respondents to the survey.

Implementation advancement

Most of the interviewed organisations have started the BCBS 239 implementation project.

The following tables show their own assessment of the advancement of the project:



Category explanations and observations:

Category	Observations
Governance • How are the different governance forums (Data, Design Authorities, Funding etc.) being brought together to support the governance of BCBS 239 delivery?	• Whilst the majority of programmes has set up governance, the integration to existing forums is limited • Governance is advanced around data management but not yet always integrated in the business or at management level
Engagement with regulators • To what extent has the bank engaged with respective supervising bodies and what are the remediation plans in place?	• Engagement varies depending on regulator/host regulator • Clear inconsistent approach so far, but this is likely to change soon
Plan definition • What is the state of preparation of detailed remediation plans?	• High-level plans are largely in place, but the level of underlying detail and understanding of dependencies is still lacking in some cases. Milestone tracking
In-flight programmes • To what extent are in-flight programmes being managed within, or as dependencies to, the BCBS 239 programme?	• Recognition that in-flight programmes are the best way to accelerate progress • Still unclear in some banks how in-flight programmes are governed and how the project portfolio is managed
Funding • To what extent is the funding case defined and does this include the requirement to support a multi-year programme?	• Significant investments in both IT and Finance related projects, however so far only allocated on an annual basis • Greater recognition that commitment to multi-year funding is required
Programme infrastructure • What consideration has been given to support infrastructure e.g. process mapping tools, data control tools, and data models to support the BCBS 239 programme?	• Limited focus on infrastructure, e.g. process modelling, data models • Some of the participants developed internal mapping tools and programme tracking models embedded within a centralised standard framework
Mobilisation • To what extent has the bank started to ramp up activity and how do they see resources being fulfilled- internally or externally?	• Project teams are being mobilised utilising a range of skills and sources • Some specifics functions are still affected by lack of budget and resources • Most of the banks interviewed anticipated that despite ramping up their resources, they will not be able to meet the deadline, and some are forecasting an additional 2-3 years of work

Compliance assessment

The following elements represent the vision of banks on their own current compliance status toward BCBS 239 principles.

Progress on governance
Most European banks declare advancement on governance from the mid-2014 survey. This means that governance principles have now been understood and are being implemented. However, reports are often pushed from the operational teams to the management, while the requirements should come from the top.

Data architecture and IT infrastructure are still weak points
If taken as part of larger scale transformation, banks can leverage BCBS 239 compliance to impact positively the whole organisation. The creation of a common data dictionary between Risk and Finance is still a distant target for too many firms.

Risk data aggregation capabilities do not demonstrate major advancement
The survey showed that banks are still struggling when it comes to defining and developing an approach to data accuracy and integrity as part of the compliance process. In addition to this, very limited progress has been made in documenting risk data aggregation processes.

Risk reporting practices reveal an approach to target compliance instead of transforming the organisations
Banks need to enhance their efforts to secure the fact that the current data, processes and systems ensure not only compliance with the requirements, but also a shift in the cultural approach to data.

From a ‘tactical fix’ to a ‘strategic build’ approach

In a strategic approach, BCBS 239 compliance is part of larger scale transformation projects that banks use as opportunities to leverage and that have significant positive impacts on the organisation.

1 Internal risk management

- Stress testing
- Internal risk modelling
- Risk reporting

2 IFRS 9

- Risk data quality
- Data availability
- Reconciliation risk/accounting

3 Capital

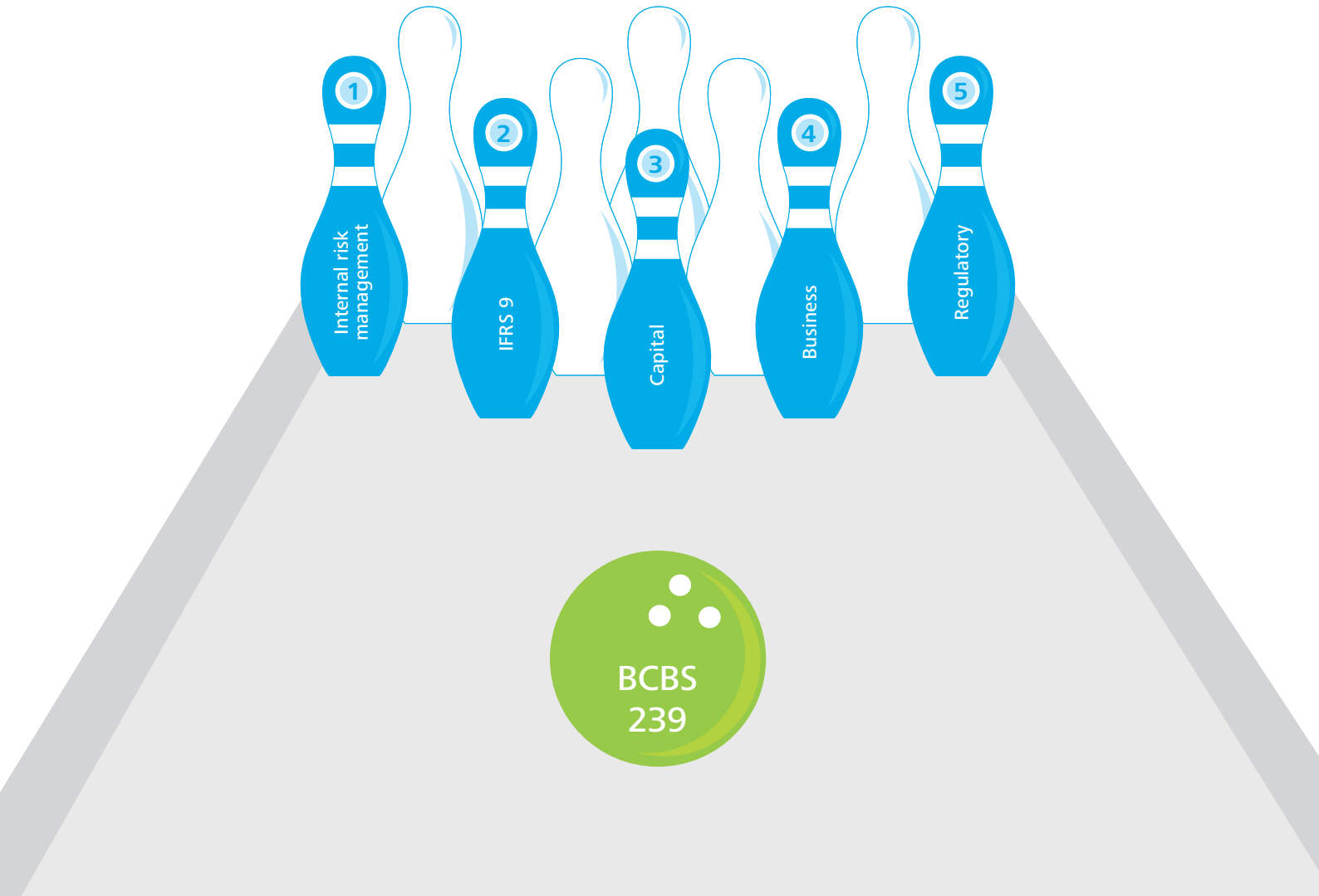
- Capital planning
- Risk bearing capacity
- Provisioning IFRS 9 impact during transitional period

4 Business

- Business Model
- New products
- Pricing
- Risk (appetite) framework

5 Regulatory

- Regulatory reporting
  - FinRep
  - Leverage
  - Unencumbered
  - Liquidity
  - Prudent value
  - Solvency
- Structure
  - Structural reforms
  - Resolution & recovery planning
- Adjustment of credit models
  - Widespread use of credit models
  - Fair value



Targeting the compliance should not prevent the banks from taking the small steps to high business value impact. Indeed, the adoption of a data management framework, for example, can help banks to leverage efficiently from regulatory obligations to operational gains.

In addition, transforming the whole organisation to be data driven and aware of the data quality at every process step will bring far more value than only focusing on risk data, e.g. when using client and contract data in customer next best action models.

Along with this, changing IT infrastructure and the applications landscape should lead to further reflections on the use of new technologies, such as digital channels enablers or data lakes. This will be a decisive factor for leading banks which aim at staying ahead of the pack in the future.

In most organisations, data architecture and IT infrastructure need to be implemented across the bank and not just for the risk function