December 2015, re-issued in May 2024

REPLY AVANTAGE

Achieving BCBS 239 compliance

A challenge not just for G-SIBs

White Paper

THE AUTHORS

Magdalena Murawska, Head of Data Practice, Avantage Reply (Luxembourg)

Magdalena is a seasoned project manager with over 15 years of experience in regulatory risk and compliance management. Her experience spans credit and market risk monitoring and reporting, risk and compliance target operating models, frameworks, and governance.

Since joining Avantage Reply in 2019, Magdalena has led multiple regulatory compliance gap analyses and advised on the remediation actions in both the banking and insurance industries. During these projects, she has developed an in-depth understanding of regulatory compliance, particularly the BCBS 239 Principles as implemented in Europe.

Throughout her career, Magdalena has successfully managed and delivered large-scale projects across various functional areas, including Client Services 1LoD, Risk and Finance. She has supported remediation programs and led system or data migration initiatives.

Currently, Magdalena leads the Compliance and Data practices in Luxembourg.

Currently,Magdalena leads the Compliance and Data practices of Avantage Reply (Luxembourg).

Magda Mirica, Head of Data Practice, Avantage Reply (Belgium)

Magda is a senior manager specialising in data governance and data strategy, with over 20 years of experience in data management, process management, communication and project management across various industries and geographies. She has supported the definition, implementation and monitoring of regulatory projects such as BCBS 239 and GDPR, as well as data quality, data governance and reporting frameworks.

Since joining Avantage Reply in 2021, Magda has advised and contributed to data management remediation programs in various banks in Belgium and Luxembourg, interacting with internal stakeholders in the first, second and third lines of defence.

Magda has covered data capabilities at operational, tactical and strategic levels, supporting remediation programs, data transformation, data governance, and data management initiatives. Her expertise has consistently added value to different client organisations.

Magda leads the Data practice of Avantage Reply (Belgium).

About **Avantage Reply**

Established in 2004, Avantage Reply (a member firm of Reply) is a pan-European specialised management consultancy delivering change initiatives in the areas of Compliance, Finance, Risk and Treasury.

TABLE OF CONTENTS

Please note that this brochure, originally published in December 2015, has not been updated to reflect any changes in regulations since that time. While the information presented was accurate as of the original publication date, it may not account for recent regulatory developments as of May 2024.

Introduction

In January 2013, the Basel Committee on Banking Supervision (BCBS) published the "Principles for effective risk data aggregation and risk reporting". The principles are designed to address the difficulties institutions face in aggregating risk exposures quickly and accurately, as well as identifying risk concentrations at the group level and along business lines. The principles were developed in response to the financial crisis, when it was revealed that many banks relied on out-of-date information technology and data architecture that failed to meet the demands posed by wide-ranging financial risks[1]. The crisis also demonstrated the need for increased reporting of economic and regulatory capital consumption, as well as stress and scenario analysis. The execution of the asset quality review (AQR) and the subsequent stress testing by the European Central Bank (ECB) and the European Banking Authority (EBA) in 2014 is another example of the necessity for integrated interaction.

The so-called "BCBS 239 paper" creates new and far-reaching demands for financial institutions and their risk management strategies. Fundamentally, the BCBS 239 positions risk data aggregation as a top-level business issue, so it cannot be treated as solely an IT concern. Because of its vast scope and its impact on data aggregation governance, architecture and processes, there is no easy route to BCBS 239 compliance.

The principles must be implemented within staggered timeframes, depending on whether a bank is classed as a global systemically important bank (G-SIBs) or a domestic systemically important Bank (D-SIB). All G-SIBs must implement the principles by January 2016, with the final nomination of D-SIBS expected in 2016. These D-SIBs will have to be compliant with the principles three years after nomination. However, in 2014, 14 out of the 37 banks surveyed (31 G-SIBs and six other large banks) indicated that they will not fully comply with at least one principle by the deadline.

While BCBS 239 implementation is proving daunting for many institutions, we maintain that full compliance can be achieved with intelligent approaches to data management and organisational change. We have developed systems that allow our clients to categorise, connect and manage their data so as to build a data architecture properly rooted in the business community. We also help institutions to explore meaningful change management. Full BCBS 239 compliance requires shifting from a siloed approach to strong integration and cooperation, particularly between the Risk and Finance departments.

Banks that meet the requirements of BCBS 239 stand to gain significant benefits. They will be able to make better judgements informed by more thorough and timely risk analysis. These banks will also be more stable in the face of uncertainty, as they will be able to quickly identify and aggregate data from across their banking group, including multiple subsidiaries and legal entities.

Avantage Reply and Xuccess Reply developed this paper to guide banks – including D-SIBs and others that wish to benefit – as they prepare for BCBS 239 compliance over the coming years. The paper provides an overview of the BCBS 239, including its objectives and requirements, along with some of the stumbling blocks identified by the surveyed G-SIBs and D-SIBs so far. Finally, the paper identifies key areas for successful BCBS 239 compliance, and looks at how banks can use the requirements outlined in the principles to their competitive advantage.

1 Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting, January 2013.

BCBS 239 requirements and objectives

BCBS 239 emphasises the fundamental principles of data management: completeness, timeliness, accuracy and adaptability. It asserts that banks should be able to aggregate their risk data across multiple business lines and be able to regularly measure and monitor the comprehensiveness of that data. The principles also seek to address a glaring issue revealed during the financial crisis, when it was found that some banks took over a month to assess their exposure risks. To this end, BCBS 239 expects banks to be able to generate reports quickly and precisely, with an appropriate balance between automation and qualitative judgement.

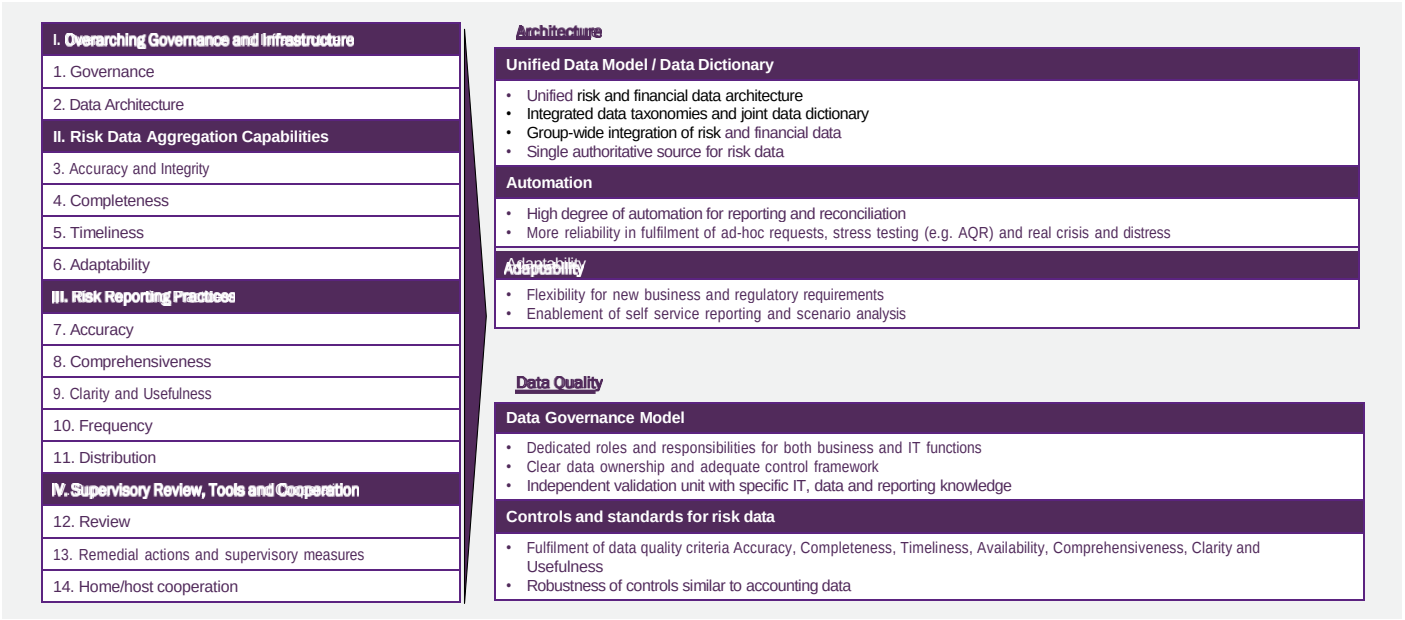
The principles are grouped under four main categories: Overarching Governance and Infrastructure, Risk Data Aggregation Capabilities, Risk Reporting Practices, and Supervisory Review, Tools and Cooperation.

I. Overarching Governance and Infrastructure: this category provides definitions of a strong governance framework, risk data architecture and IT infrastructure.

II. Risk Data Aggregation Capabilities: these principles stipulate that banks should generate accurate, reliable and up to date risk data across the banking group activities in order to identify and report risk exposures, concentration and emerging risks. Notably, the principles under this category represent central challenges for banks' corporate structures – all these principles demand prioritising risk data aggregation at the business level, rather than remaining solely an IT concern.

III. Risk Reporting Practices: this category is concerned with the continuous improvement of reports and creating clear lines of responsibility. The principles are designed to ensure that reports are accurate, convey aggregated risk data and are reconciled and validated. Under these principles, reports should also be comprehensive, clear, useful and set on a frequency that meets recipients' requirements.

IV. Supervisory Review, Tools and Cooperation: this category outlines how supervisors should review and evaluate banks' compliance to these principles. As this white paper is focused on achieving compliance for institutions, it covers only the first three categories (i.e. principles 1–11).



Changes and main objectives

The key objective of the BCBS 239 is to improve banks' abilities to respond to the risk environment and to generate accurate, timely and comprehensive reports that inform business judgements. This includes improving the reporting infrastructure, enhancing Group-wide decision-making processes, accelerating the production of ad- hoc and standard reports, and refining strategic planning and risk management. Ultimately, these initiatives are designed to reduce the probability and severity of losses experienced by banks.

It is often assumed that BCBS 239 is only significant and relevant for the IT landscape, data integrity and risk reporting dimensions. From our perspective, a more comprehensive strategy is required to generate high internal added value. Such an approach requires the integrated interaction of processes, corporate governance, data governance and data quality, business content and banking group wide organisational structures, including their continuous improvement.

As such, the BCBS 239 has wide-ranging impacts on organisations' business operations, including:

Governance: The BCBS 239 shifts risk data aggregation and risk reporting responsibilities far beyond the IT department. The principles call upon the board and senior management to take ownership for their organisation's risk data aggregation capabilities and risk reporting practices, and to ensure that dedicated roles for both Risk and IT functions are in place. Enterprise-wide understanding of the data architecture and resilience to change mean that the approach to compliance must be sustainable.

Infrastructure: In order to comply with the principles, many banks will be required to overhaul their dated IT infrastructure. BCBS 239-ready infrastructure should enable full and traceable documentation, and clear and comprehensible data lineage. Automation should be the dominant process, with limited manual interventions and workarounds required. Data aggregation and reporting possibilities must be flexible enough to respond to a wide range of requirements, including demands posed by new regulations, such as AnaCredit and IFRS 9.

Data Quality: Banks must measure the quality of their data at every level of the supply chain. However, measurement on its own is insufficient – banks must also implement programmes that address quality concerns promptly and efficiently. Again, the board / top management level should prioritise these data quality issues.

Reporting: Banks are also required to demonstrate the robustness and timeliness of their reporting capabilities. Automated reporting is preferred to reduce the possibility of human error.

The Principles (1-11)

I. Overarching Governance and Infrastructure

1. Governance

A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other principles and guidance established by the Basel Committee.

The bank's board and senior management should take on high levels of involvement and responsibility, ensuring that data quality risks are part of a strong risk management framework. Senior management should also be aware of any limitations within the bank that prevent full risk data aggregation and promote a supporting IT strategy to overcome impediments.

These risk data aggregation capabilities and risk reporting practices should be thoroughly documented and be subject to a high standard of validation. The capabilities and practices should be independently verified, and critically assessed as to whether they are performing appropriately and in line with the bank's risk profile. and in line with the bank's risk profile.

In addition, risk data aggregation capabilities and reporting practices should be considered as part of the due diligence process of material acquisitions, as with any other new initiatives or change processes.

Good governance and good infrastructure are closely related in the BCBS 239 – indeed, a strong governance structure can oversee the development of robust and high-performing data architecture and infrastructure. As such, principle 1 is fundamental to the success of the remaining principles.

2. Data Architecture and IT infrastructure

A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices, not only in normal times but also during times of stress or crisis, while still meeting the other Principles.

While banks do not necessarily need to have a single data model, data taxonomies and architecture should be strongly integrated across the banking group. Standardised identifiers and/or naming conventions should be used for data across the group, including legal entity, counterparties, customers and account data. Clear roles and responsibilities related to Data Quality Management should be established within Business and IT functions. Finally, data taxonomies and architecture should also be integrated with the bank's Business Continuity Management (BCM) software and Business Impact Analysis (BIA) processes.

This means that ensuring stable conditions and the creation of a robust but agile data structure, model and architecture are more critical for success than new technology. Top-level management support and business involvement needs to be guaranteed in this process. BCBS 239 is not solely an IT concern – rather, it is critical to overall business and management.

II. Risk Data Aggregation Capabilities

3. Accuracy and Integrity

A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors.

BCBS 239 underlines that banks need to have clarity across the organisation and standard definitions of terms. To this end, a bank should maintain a 'data dictionary' clearly outlining the concepts used. The controls around risk data should be comparably robust to those applied to accounting data. Banks should also seek to have one authoritative source for risk data for each type of risk.

Banks need to ensure that the appropriate personnel have the required access to the risk data and are able to report risks in an accurate and timely fashion. An appropriate balance between automated and manual systems should be maintained, with a high degree of automation (so as to avoid human error) supported by human intervention when necessary. While the Supervisor permits manual workarounds, these processes must be rigorously documented. Data accuracy should be continually measured and monitored, with action plans in place to rectify poor data quality.

Principle 3 has represented a serious challenge for banks, with a particularly low level of compliance reported. This stems in part from the fact that standard accounting-like controls, used previously by many banks, treat risk and accounting systems separately. To comply with Principle 3, banks need to shift their focus towards joint data quality management, with risk and accounting systems properly integrated.

To achieve this, banks should use a common standard for the data dictionary e.g. the Financial Industry Business Ontology (FIBO).

4. Completeness

A bank should be able to capture and aggregate all material risk data across the banking group. Data should industry, region and other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, concentrations and emerging risks.

As such, a bank's risk data should be materially complete with any exception identified and explained. This should include off-balance sheet exposures. A common metric or basis is not required, however risk data aggregation capabilities should be the same.

Pre-loading all relevant data on a granular level into the data store is recommended. However, maintaining and linking collateral management data represents a special challenge.

5. Timeliness

A bank should be able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, set based on the characteristics and overall risk profile of the bank.

These capabilities should ensure that the bank is able to produce risk data on a timely basis – this includes the production of rapid risk data to assess critical risk in a stress or crisis situation.

Such critical risks include, but are not limited to:

- Credit exposures to large corporate borrowers;
- Counterparty credit risk exposures;
- Trading exposures, positions, operating limits, and market concentrations by sector and region data;
- Liquidity risk indicators; and
- Operational risk indicators that are time-critical.

Critical risk data should be given priority in establishing the data model. In addition, many banks need to shift away from manual processes and interventions for generating aggregate risk data, as this impedes a bank's ability to respond promptly in times of crisis.

6. Adaptability

A bank should be able to generate aggregate risk data to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries.

This capability should enable scenario analysis and quick decision-making, and support data customisation (such as dashboards and risk summary reports). The aggregate risk data should also be able to quickly incorporate business developments, external factors and regulatory changes.

Again, this area has proven remarkably difficult for G-SIBs and D-SIBs, with 10 (possibly 11) of the banks surveyed reporting anticipated non-compliance with Principle 6. In order to meet compliance, the design and configuration of risk reports should become primarily a business task, with additional support from IT.

Overall, the Risk Data Aggregation category represents a key challenge for banks. Slightly less than one third of all banks surveyed in 2014 expect that they will not be compliant with Principles 3, 5 and 6 by January 2016.

III. Risk Reporting Practices

7. Accuracy

Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.

To ensure accuracy of reports, banks will be required to have defined requirements and processes to reconcile reports to risk data. It is also expected that banks will have automated and manual edit and reasonableness checks, including an inventory of the validation rules that are applied to quantitative information. In addition, banks should ensure that they have integrated procedures for identifying, reporting and explaining data errors or weaknesses in data integrity via exceptions reports.

Supervisors will also expect banks to establish expectations for the reliability of approximations, and accuracy and precision requirements for both regular and stress/crisis reporting.

The overall data quality management (DQM) process should be linked to the metadata management programme. Data quality checks need to be embedded in the DQM system, with remediation of errors tracked in a ticket system.

8. Comprehensiveness

Risk management reports should cover all material risk areas within the organisation. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients.

Risk management reports should include exposure and position information for all significant risk areas, i.e. market, credit, liquidity and operational risk. They should also identify emerging risk concentrations. A typical aggregated risk report should include, at a minimum: capital adequacy, regulatory capital, capital and liquidity ratio projections, credit risk, market risk, operational risk, liquidity risk, stress testing results, inter- and intra-risk concentrations, and funding positions and plans.

An iterative approach to data management implementation is recommended to ensure achievable results and operationalisation.

9. Clarity and Usefulness

Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include meaningful information tailored to the needs of the recipients.

To this end, reports should maintain an appropriate balance between risk data, analysis and interpretation, and qualitative explanation – it is expected that the higher up within the organisation, a greater the degree of qualitative interpretation will be required.

It is also crucial that banks develop an inventory and classification of risk data items.

10. Frequency

The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed, at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis.

Naturally, the frequency of risk reports will vary according to risk type, purpose and recipients – banks should routinely assess the purpose of each report and whether its frequency is appropriate. Some position/exposure information may be needed immediately (intraday) in periods of high stress.

Determining the frequency of report production should be a high-level management activity. The chosen frequency should be responsive to the purpose of the report and the situation at hand. As with principle 5, banks should focus on eradicating manual processes and workarounds in producing critical risk data.

11. Distribution

Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained.

A consistent, role-based security concept is required to ensure the 'need to know' principle can be adhered to.

Main Challenges for compliance

While the BCBS 239 itself is not lengthy, compliance has proven enormously challenging for banks. These difficulties stem from the BCBS 239's wide-reaching requirements, which can radically alter how banks manage their data lineage, architecture and governance structures.

Some firms demonstrated an over-reliance on existing purpose-built infrastructure and reporting capabilities. A large number of banks still rely on manual workarounds. For many of these organisations, these processes are out-of-date and relatively unsophisticated, requiring cumbersome data 'cleansing' and manual calibrating before aggregation can take place. Remarkably, some of these firms rated their compliance with the reporting principles higher than their compliance with the governance, infrastructure and data aggregation principles. Some firms appear compliant at the Group level or at the level of a specific legal entity – but lack the same capability at different aggregation levels. In this sense, these firms fail to meet the adaptability requirement.

Some firms are preoccupied with large-scale in-flight projects spanning 2016 and beyond. For these banks, the resources are simply not available, while the data landscape is continually changing. A piecemeal approach to compliance – driven solely by the IT department, or limited by project resources, rather than stemming from holistic structural change – means that compliance, once achieved, may not be sustained.

Fundamentally, this lack of readiness stems from the absence of a sustainable embedded enterprise-wide understanding of the data landscape – and the business context in which it operates. Too often, data aggregation and reporting have been siloed as IT concerns, while the BCBS 239 requires a holistic approach connecting risk, finance, IT and business operations. These banks need to prioritise the governance/infrastructure principles as a precondition for achieving full compliance should ensure that they have integrated procedures for identifying, reporting and explaining data errors or weaknesses in data integrity via exceptions reports.

Supervisors will also expect banks to establish expectations for the reliability of approximations, and accuracy and precision requirements for both regular and stress/crisis reporting.

Solutions and benefits of compliance

This section provides an overview of what banks need to do to achieve BCBS 239 compliance, and how any implemented changes can be made sustainable. Based on our experience with a number of institutions, we have identified the four key areas that banks need to focus on. We have also developed a three-step solution for data management that helps banks organise their data for BCBS 239 compliance, and a modular-based approach to change management that ensures that the principles are properly implemented across all levels of an organisation.

Four main areas of focus for compliance

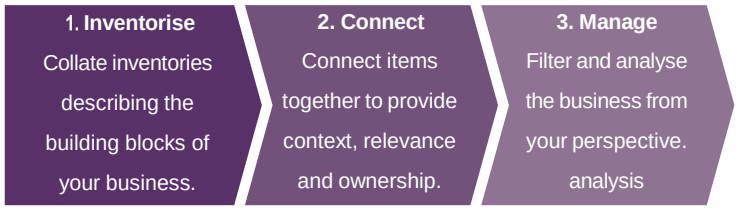
Organisations must consider the following four key areas of activity when commencing to work towards BCBS 239 compliance. These activities must be addressed through a departmental and cross-divisional cooperation approach in order to meet the requirements.

AREAS OF ACTIVITY FOR BCBS 239 COMPLIANCE

Processes	• Accelerate ad hoc and standard reports through a structured report creation process • Define quality gates for content • Define clear responsibilities for processes within Business, Risk, Finance and IT functions
Data management	• Develop an integrated, agile and Group-wide data budget • Define data quality measures • Define clear responsibilities for data quality management within Business, Risk, Finance and IT functions
Governance	• Create a Risk Management Framework and Data Quality Framework • Integrate frameworks into the annual review process and Group Guidelines • Develop validation concepts for risk data and reports
Organisation structure	• Break the “silo” and minimise operational risks through targeted development of Human Factors

Our three-step process for BCBS 239 compliance

Once the above four areas have been identified, organisations should engage in a systemic process that ensures compliance with the principles. Our three-step solution allows banks to methodologically implement the principles in a holistic way – this means that changes have lasting, meaningful impact. This section provides a brief overview of the process.



Step 1: Inventorise

Step 1 involves creating an inventory of the key objects making up the firm's data aggregation capability in an incremental fashion. This requires categorising risk data elements, identifiers and data definitions – both in standardised form and in their representations in specific systems.

As with all elements of the BCBS 239, strong governance is required in this process. Roles and responsibilities for risk data must be determined at each stage in the data aggregation and reporting lifecycle.

Robust and up-to-date infrastructure must be established that is capable of the required data transformation and aggregation processes, including both automated processes and manual interventions.

Reporting output should also be clarified at this stage, including coverage, content, distribution and purpose.

Step 2: Connect

The second step involves connecting the objects above (the 'data dictionary'), and making them visible in an integrated way across the organisation. Information about this data landscape must become corporate understanding that is embedded and actionable – sustainable through collaboration by business and IT owners. The data elements must be located in the real business context – related to people, policies and processes within the organisation.

Data lineage and data aggregation must be visible and understandable to all stakeholders throughout the lifecycle from data capture to reporting.

Step 3: Manage

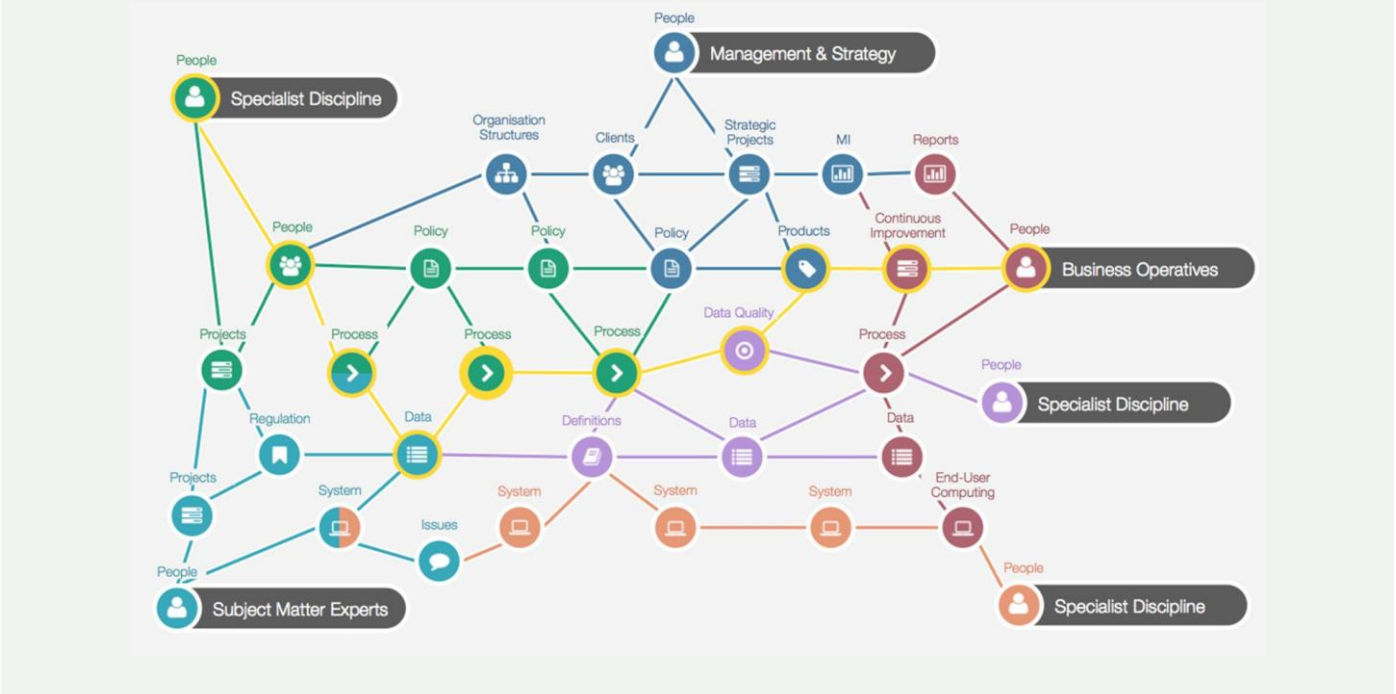
The final step requires managing the corporate understanding developed above so that it remains current and correct. Business owners of data and process must remain responsible for content. At Step 3, it is also vital to ensure that key stakeholders – e.g. decision-makers and independent validators – can access the required information. This step ties in strongly to organisational change management processes, outlined below.

Overall outcome: Data architecture located in the business community

The ultimate aim of the above processes is to inform the design of a data architecture firmly rooted in the business community.

Data architecture captured in project-generated and system-level documents or spreadsheets is neither usable nor sustainable. To create a compliant solution, organisations must build data understanding incrementally, using a web-delivered toolset that supports collaboration among the community of business owners, decision makers and change managers.

Both **Avantage Reply and Xuccess Reply** work with our specialist partner, Axon, to help our clients develop effective metadata management. Axon provides special software that simplifies data flow and transparency of business context of data accross entreprise.



Source: Diaku

Change management: the ultimate factor for success

BCBS 239 is far more than a 'box-ticking' exercise. To achieve full compliance and ensure the maximum benefits, we recommend that organisations adopt a programme of 'cultural change'. This programme should underpin the implementation of the above four areas: processes, data management, governance and organisation structure. Prioritising cultural change will ensure the required take-up of BCBS 239 at all levels of the organisation, and reduce the chance of implementation being a piece-meal exercise.

Importantly, BCBS 239 requires strong cooperation between the Risk Management and finance functions. An effective change management programme for BCBS 239 breaks the silos and brings these two functions together to allow an integrated approach to compliance.

We have worked closely with a number of institutions to facilitate the necessary cultural change required for the successful implementation of new regulatory frameworks.

Benefits of BCBS 239 compliance

Implementation of BCBS 239 poses major demands for banks in terms of resources, costs and upheaval in terms of the interaction between organisational units. These difficulties should not be without benefit. In complying with the principles, banks have the opportunity to create efficient processes and IT architectures for modern bank management. By having consistency of data, and the ability to quickly generate accurate, informative and meaningful reports, banks will be well placed to act on the business landscape and develop a competitive advantage.

SOLVING EVERYDAY CHALLENGES – SOME EXAMPLES

Issue	How to address through BCBS 239 compliance
Lack of communication between departments	Cross-functional impacts can now be traced and visualised Better alignment of risk and accounting departments means fast production of report and metric implementation, along with better coordination of key processes (liquidity coverage ratio, risk-weighted asset production, etc.)
Fragmentation	Local terms are mapped on into a central glossary to allow a two-way translation Data can be aggregated on geographical/regional, legal entity, industry, asset class and business line levels
Manual workarounds	Greater insight into manual workarounds and their impact on the data architecture Higher level of automation reduces risk of human error and improves expediency Reduced cost of manual workarounds
Multiple data warehouses and platforms	Data lineage and disconnects are made obvious Reduction of IT costs through standardisation of data assets and tools
Changing architectures	Data lineage and disconnects are made obvious Reduction of IT costs through standardisation of data assets and tools
New requests from regulators	Banks are in a better position to meet changing regulatory requirements (ex: Anacredit)

Conclusion

BCBS 239 represents a serious challenge – for G-SIBs, D-SIBs and other institutions. Many D-SIBs will face compliance over the coming years. Given the difficulties faced by G-SIBs so far, it is vital that D-SIBs and others that wish to meet compliance should begin preparing now. As highlighted, this cannot be achieved through a simple 'box-ticking' process, as the principles have ramifications for the very highest levels of business and governance. Institutions that recognise this, and that implement effective programmes of change management and governance improvement, will be in a much better position to meet the requirements of BCBS 239.

While certainly demanding, the BCBS 239 stands to bring significant benefits to banks that successfully comply. More than simply a regulatory exercise, the principles will allow banks to develop more robust, agile and standardised risk data management. These banks will be able to respond quickly and accurately to crisis situations, along with meeting requests from regulators and clients. It is an opportunity for banks to break Risk and Finance silos, and develop a more modern, responsive and integrated approach. As such, following the principles is a worthwhile investment.

CONTACTS

Avantage Reply (Brussels)

5, rue du Congrès
1000 Brussels
Belgium
Tel: +32 (0) 2 88 00 32 0
E-mail: avantage@reply.com

Avantage Reply (London)

Nova South, 160 Victoria
Street, Westminster,
London SW1E 5LB
United Kingdom
Tel: +44 (0) 207 730 6000
E-mail: avantage@reply.com

Avantage Reply (Luxembourg)

21-25, Allée Scheffer
2520 Luxembourg
Luxembourg
Tel: +352 28 68 43 1
E-mail: avantage@reply.com

Avantage Reply (Milan)

Via Castellanza, 11
20151 Milano
Italy
Tel: +39 (0)2 535761
E-mail: avantage@reply.it

Avantage Reply (Paris)

33, rue des Châteaudun
75009 Paris
France
Tel: +33 (0) 170 23 08 74
E-mail: avantage@reply.com

Avantage Reply (Germany)

Uhlandstr.2
60314 Franckfurt am Main
Germany
Tel: +49 (0) 69 9999937-0
E-mail: avantage@reply.com

Avantage Reply (Rome)

Via Del Giorgione, 59
20151 Roma
Italy
Tel: +39 (0)6 844341
E-mail: avantage@reply.it

Visit Avantage Reply's LinkedIn page

REPLY AVANTAGE