

**BCBS #239: the transformation
towards the compliance**

Based on Deloitte's EMEA Survey
September 2017

Introduction

Since January 2016, G-SIBs have been working to deliver the remaining components of their strategy comply with the 11 principles for effective risk data aggregation and risk reporting. However, the **latest annual progress report**, published by the Bank of International Settlements (hereafter BIS) in March 2017, indicated **several weaknesses** for the 30 G-SIBs analysed. The questionnaire highlighted that these banks have failed to reach the target level of compliance. None of the banks analysed has been able to achieve full compliance on any of the 11 principles, and several of them are still “materially non-compliant” on most of the principles (in particular Data architecture and IT infrastructure reported the lowest score). For this reason, the Committee has requested banks to provide an **updated detailed roadmap**, in order to address the main challenges identified. In addition, the BIS asked **D-SIBs to define and recalibrate their approach to compliance** with the regulatory principles. Banks should leverage the approach used by those peers with plans in more advanced state of completion and define a new path towards full compliance. Mainly, they need to capitalise on the lessons learned by the industry, in order to define a reliable timeline for achieving significant progress and comply with the regulatory deadline.

Evolution of compliance: main challenges

The main dilemma that banks faced during the mobilisation and planning phase of their bespoke **BCBS #239 compliance programs** was the one over **different approaches, "Fix" or "Build"**. Banks had to choose between a "soft" **program of adaptation of existing infrastructures and processes** to be compliant with regulatory requirements, or **more cumbersome programs** with a strong innovative connotation **based on several organizational, infrastructural and technological interventions**. The wide range of activities foreseen, and the tight timeframe available for implementing the principles of the regulations, encouraged the banks to follow mainly a tactical approach, in order to maximise the results achievable in the existing timeframe. This was mostly due to the fact that a path to full compliance considering an integrated strategic and technological approach would require a longer time horizon to implement.

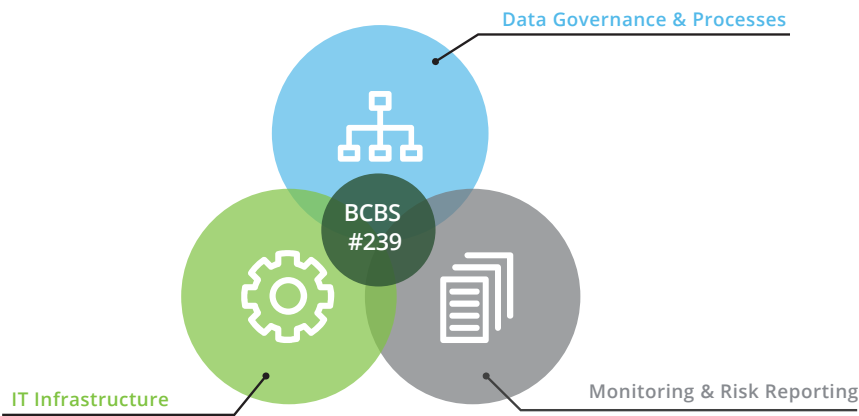
In order to meet the Regulator's requests, it's vital to develop a **plan that takes into account the entire risk reporting value chain**; this means considering **risk data as an asset** that has to be **accurate, clear, complete and easily available**. Some banks, underestimated the planning effort, having to revisit the project scope during the course of their programs.

Banks have complex and structured organizations, the result of a stratification of business decisions and acquisitions



over several years. This has historically resulted in an approach to risk monitoring always considered (even by the Regulators themselves) as "silos-based" instead of "cross risk" as outlined by the new ECB rules (i.e. Comprehensive Assessment). Financial institutions need to avoid a "siloesd" approach in order to reflect the interconnected nature of risks and allowing them to manage the evolving regulatory landscape.

BCBS #239 aims to break down the "siloesd" approach, where every risk is monitored individually, without having a common aggregated view of the counterparty exposure. This is crucial in order to avoid underestimations within the risk monitoring processes that could prevent the effectiveness of the control.



In order to **achieve compliance**, banks identified different aspects that can be summarised by the **following three drivers**:

Governance and Process

A “siloesd” view has generated an accountability spread across functions and levels, preventing the definition of a clear process that starts from Group-wide Top Management’s decisions and trickles down to the legal entities at local level. Banks do not have a clear and formalized definition of roles and responsibilities. The absence of an organizational model results in non-coherent and redundant processes. Therefore, the new supervision framework must avoid activities’ duplication and inefficiencies in order to set up more streamlined and timely processes.

IT infrastructure and data aggregation process

In order to assess the risk-data aggregation capabilities, a key step is the documentation of each risk metric including, for example, its related risk data, data lineage, responsible organizational unit, type of risk process (manual/ automatic), type of system (end-user/ application), controls, pain points and root causes. Multiple data models and data taxonomies across legal entities and risk types were merged in a unique data model and data dictionary consolidated across the institutions, ensuring the identification of the “golden source” through the data

lineage. It is also important to create an infrastructure that supports the implementation of automatic data quality checks and reconciliation processes. Indicators and trend analysis will become fundamental metrics of report accuracy and will render manual cleansing marginal, delivering more consistent data for the new cross-risk views and reports.

Risk reporting

The old regulatory approach led banks to generate reports aggregated from multiple systems, with rigid standards and predefined frequencies. In order to move towards a compliant process for the production of comprehensive risk reports, banks have to consider the granularity of the metrics, eliminating redundancies, improving timeliness and reporting accuracy, thus easing validation process.

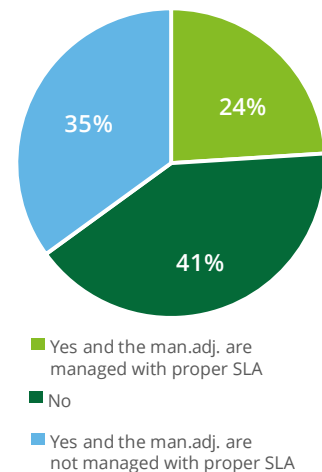
The latest assessment on the banks compliance level, shows that there are still several open actions and many challenges to be addressed in order to fully comply with the requirements. Banks continue to face challenges in terms of:

- Management of complex projects that involves strong organizational, architectural and technological interventions;
- Difficulties in removing manual intervention in the generation of risk reports;

- Definition of an effective Data Quality Framework allowing the identification of anomalies and enabling the monitoring of data quality;
- Incomplete integration and implementation of data architecture and frameworks (data taxonomies, data dictionaries, risk data policies);
- Definition of rules for a well-known distribution process of the reports and design of each report.

These challenges are also highlighted by the results of the **Deloitte 2017 Survey** that involved 18 banks across EMEA. In fact, 80% of banks in the sample claimed a compliance level between 75% and 100%. However, this only tells one part of the story. A further analysis reveals that the reporting production still involves manual adjustment activities, sometimes using different IT sources (the scenario generation requires a greater effort on data production than data analysis). Consequently, new investments are required in order to fully automate the data production process. Furthermore, 59% of surveyed banks have created an End-to-End Data Quality monitoring tool, but only in 24% of cases the manual adjustments are managed with proper SLAs¹ (Figure 1).

Figure 1 | Has a E2E Data Quality monitoring tool been created? If yes, are the manual adjustments managed with proper Service Level Agreement (SLA)?



¹SLA = Service Level Agreement

Evolution of compliance: lessons learnt



The deadline defined by BCBS #239 for G-SIBs is overdue, whilst an increasing number of D-SIBs have already started programs to achieve compliance. Taking into account the different deadlines defined for G-SIBs e D-SIBs, the most important consideration about the BCBS #239 principles is the fact that these **should not be seen as a simple compliance** to regulatory requirements exercise, but as an **opportunity to develop the main pillars** (governance, data architecture, IT infrastructure, and high-quality data) in order to guarantee superior risk reporting capabilities. Indeed, one of the lessons learnt is the importance of adopting a long-term strategy with the aim of improving the key capabilities in a structured approach. This means acquiring, in future, the **ability to manage stress/ crisis situation supported by data, process and reports** with a high value and clear information. This should enable the management to take

effective decisions according to the bank's business model and risk profile. Given that BCBS#239, qualified as a principle-based regulation, it does not prescribe how to achieve compliance. Banks have adopted different approaches to compliance, which range from focusing only on the reporting process to all-encompassing initiatives involving the technological infrastructure. It was therefore difficult to compare and homogenize the results achieved by banks. In **July 2016**, national supervisors were asked to complete a **questionnaire assessing the banks' progress on compliance with BCBS#239 principles**. The results from the analysis show that **banks have not yet achieved compliance**: only one bank had achieved full compliance with the principles. Most of the banks are expected to achieve full compliance before (24 banks) or beyond (4 banks) the end of 2018. However, the **survey carried out by Deloitte shows that banks' compliance level is in line**

with expectations. In fact, 80% of banks interviewed deem to have achieved a compliance level between 75% and 100%, applying the BCBS#239 principles to the main risk areas.

In particular, the **main differences in the compliance level estimation** are related to the following features:

- **Governance & Processes:** the Deloitte survey stresses the importance that banks gave to the definition of a Data Governance framework, but the regulator assessment illustrates the need for further investments in this field;
- **IT infrastructure:** the Deloitte survey shows that banks estimate a compliance level of about 70%, however the regulator's assessment highlights the persistence of a sizeable gap against the target compliance level due to the high operational risks connected with manual adjustments.

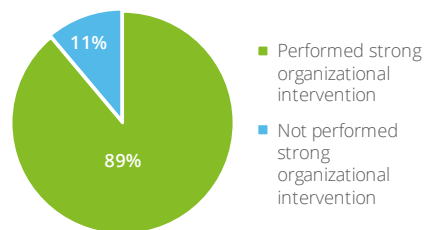
Governance and Process

The self-assessment required by the regulator, highlighted the importance of defining roles and responsibilities across the organization. In order to comply with the BCBS #239 principles, the adoption of new approaches to managing, analysing and understanding information is essential. Data must be seen as a resource for the bank, both during the decision making process as well as in communicating with external stakeholders.

The process of granting high quality level data must involve all the stakeholders, leveraging the revamped role of the Chief Data Officer (Figure 2). This figure has been empowered with greater authority to supervise the data process and support the cultural change across the whole

bank. Almost all banks included in our survey (89%) have implemented strong functional transformations including, for example, dedicated organizational structures, through the definition and the formalization of the mission, the roles and the responsibilities.

Figure 2 | Does the bank perform strong organizational interventions including, for example, dedicated organizational structures, through the definition and the formalization of the mission, the roles and the responsibilities?



Fourteen banks out of 18 have defined a new unit (Chief Data Office) that sets the rules and monitors the End-to-End data process, but only 12 provided a new cross risk unit, abandoning the “*siloes*” approach (Figure 3).

Figure 3 | A new unit (i.e. CDO), which sets the rules and monitors the End-to-End data process, has been defined as follow...

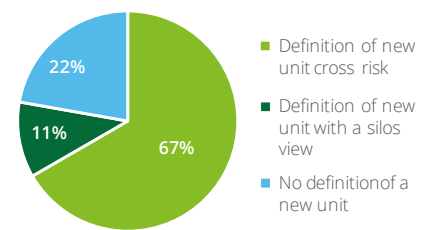
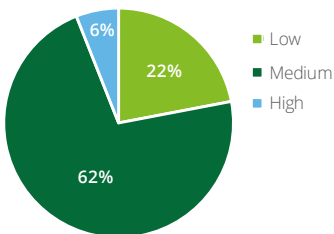


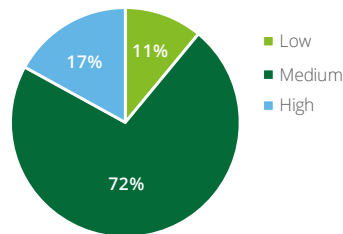
Figure 4 | Completeness, Accuracy & Integrity and Timeless

Completeness



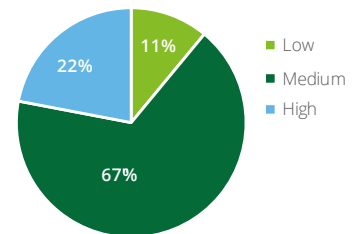
Completeness still requires **manual adjustments to aggregate data**

Accuracy & Integrity



Accuracy & integrity have been achieved by the sample. Nevertheless, **manual adjustment can produce operative risks**

Timeliness



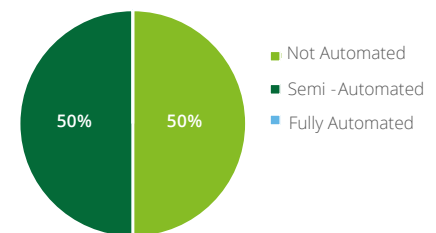
Timeliness has been achieved by the sample but they could have **some constraints in stressed situation**

IT infrastructure and data aggregation process

Banks have understood that complete, accurate and timely (Figure 4) data management is possible thanks to an IT infrastructure, an aggregation process and a data dictionary that allows for a unique taxonomy of risk data and the identification of the single point of truth. Risk data readily available, and already reconciled with the accounting information, reduces the risk of misjudgements and improves the capability of the top management to take long-term decisions based on truthful information.

Moreover, in order to support the management in the decision-making process, it is important for the level of detail of data to be consistent in order to allow for flexible aggregation and reporting. In this context, banks have started to invest in the review process (for example, data quality process), with a focus on the automation of reconciliation processes across different risk datasets. This has been set up with the aim to enhance the IT architecture. However, further progress can be achieved in automating the reconciliation processes (Figure 5) (to date it is semi-automated for the 50% of respondents to the survey).

Figure 5 | How can you judge the automation level in the existing reconciliation processes?



Investments are foreseen to improve reconciliation also for managerial purpose (before B/S closing)

Risk reporting

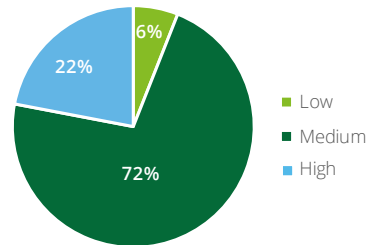
Banks need to understand the importance of developing a proper reporting framework in terms of perimeter, cross risk measures and functionalities available. On the whole a report should be:

- Useful and clear in order to guarantee the possibility for the top management to monitor risks
- -Standardised and automatically generated (Figure 6), with drill-down functionalities for a deep understanding of the various risk dimensions.

These features enable the creation, almost in real time, of “on-demand reports” for specific risk type (e.g., market and counterparty risk) and the development of an “ad-hoc” analysis for the top management, in order to take strategic decisions.

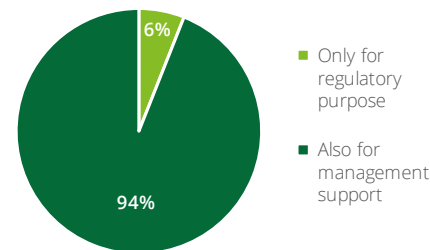
An important consideration is that these reports should not only be used to comply with regulatory requirements, but also to support the management in the decision-making process (Figure 7). This requires the creation of reports that fulfil the bank's business models and its risk profiles.

Figure 6 | Automation



Automation is **still a challenge for banks** as highlighted also in BIS assessment
Investments are foreseen by banks to improve compliance in next years

Figure 7 | BCBS #239 application on reporting...



BCBS #239 covers both managerial and regulatory reports

Recommendations

The varying approaches adopted across the industry highlighted how principles-based regulation can generate different expectations between regulator and banks over the definition of compliance.

However, some banks appear to have misinterpreted the Committee's expectations, considering BCBS #239 as a one-time compliance exercise rather than a dynamic and ongoing process. Therefore, only **considering all aspects impacted by the regulation**, and the deep-rooted operating model consequences, banks can realize benefits of BCBS #239 compliance. By adopting this approach, with a forward-looking view, banks can meet certain compliance requirements around comprehensive data and reports for other regulations, including Comprehensive

Capital Analysis and Review (CCAR), Comprehensive Liquidity Assessment and Review (CLAR), Supervisory Review and Evaluation Process (SREP) and Target Review of Internal Models (TRIM).

Banks with compliance plans already in-flight (both G-SIBs and D-SIBs) should review their approaches and undertake, if needed, some corrective actions in order to ensure full compliance. On the other hand, banks that are starting their compliance programs need to adopt a long-term strategy, leveraging the approaches that other G-SIBs and D-SIBs have implemented to achieve compliance. The aim is to define priorities according to the specific business model, considering other on-going programs and focusing on the business benefits that the compliance process can guarantee.

How the Banking Sector is approaching BCBS #239



Since early 2016, **external and internal auditors** have been carrying out **targeted reviews of banks' compliance** with the BCBS principles. In both cases, the evaluating team developed a certification procedure based on high standards of validation. Identified deficiencies have been reported, in the majority of cases, to the Board in order to ratify appropriate remedial actions. The people responsible for the areas of partial compliance have been since called to provide remediation plans, defining a reasonable timeline to close the gaps, subject to supervisory review.

As the severity of the banks' weaknesses increases, additional supervisory measures should be taken. Considering the possibility of choosing the most appropriate approach for banks to achieve compliance, the ECB – in line with its priorities – launched the **2016 Thematic Review**, in order to define the standards to be applied to homogeneously assess the compliance level across banks. The Review involved both the largest banks that fall under the SSM as well as the smaller domestic banks. **The review was structured in two phases: an**

initial assessment of the efficiency of IT infrastructure and governance, and a second phase consisting of a Fire Drill (FD) exercise and a Data Lineage exercise. The objective of the second component was the assessment of the ability to aggregate and report a dataset in an accurate, comprehensive and timely manner. The independent Internal Audit department (IA) (or Internal Validation Unit of the bank) was invited to carry out a report aimed at assessing the quality of the data reported by the bank.

Analysing further the details, the National Controlling Authorities asked the banks in the Fire Drill exercise to compile and submit, at short notice, selected indicators on leverage in a pre-defined template. The ECB also tasked the banks' Internal Audit function to conduct an independent validation of the data submission. Many Banks were not able to provide real time data during the exercise due to the complexity of the required information.

The Data Lineage exercise focused on the banks' capabilities against two risk types, credit risk (CR) and liquidity risk (LR). The exercise required to:

- Map the data lineage indicators in a flowchart
- Identify the process steps and specify if they were fully, partially or not automated
- Explain the data quality indicators provided
- Test the bank's capabilities to drill down the indicators

The exercise showed that many banks had not yet adopted a specific tool for the data lineage, or that, in some cases their reporting system does not allow for the desired level of drill down capability. Other banks have implemented or are implementing tools for Dictionary Management, Data Lineage, Quality Management and Certification, but sometimes these tools, the exercise showed, do not involve all risk data and metrics.

The outcomes of the Thematic Review has highlighted that even though G-SIBs have increased their compliance level they still have **several open points to address to improve their level of compliance**, to cover both managerial and regulatory reporting.

Links with the new regulatory requirements

In recent years, the banking system has been facing a phase of transformation, triggered by a wave of changes in risk management methodologies, requiring a greater level of detail on capital, liquidity and funding requirements as well as increased standards for risk reporting (Pillar II, AnaCredit, SREP, FRTB, TRIM, etc.) (Figure 8). The Regulator, who has now more data and insights at its disposal than ever before, uses these elements to inform the design of new regulatory requirements. The increased transparency has allowed for an in-depth understanding of the challenges faced by financial institutions and for more accurate actions aimed at limiting the spread of systemic risks potentially affecting investors and depositors, ultimately reducing the frequency of extreme measures like the bail-in.

Every bank must incorporate new rules as quickly and efficiently as possible in order to contain compliance costs. **The principle-based nature of BCBS # 239 offers an opportunity for the banking system to redefine its internal policies taking advantages of all the related benefits arising from the Risk Data Aggregation framework.**

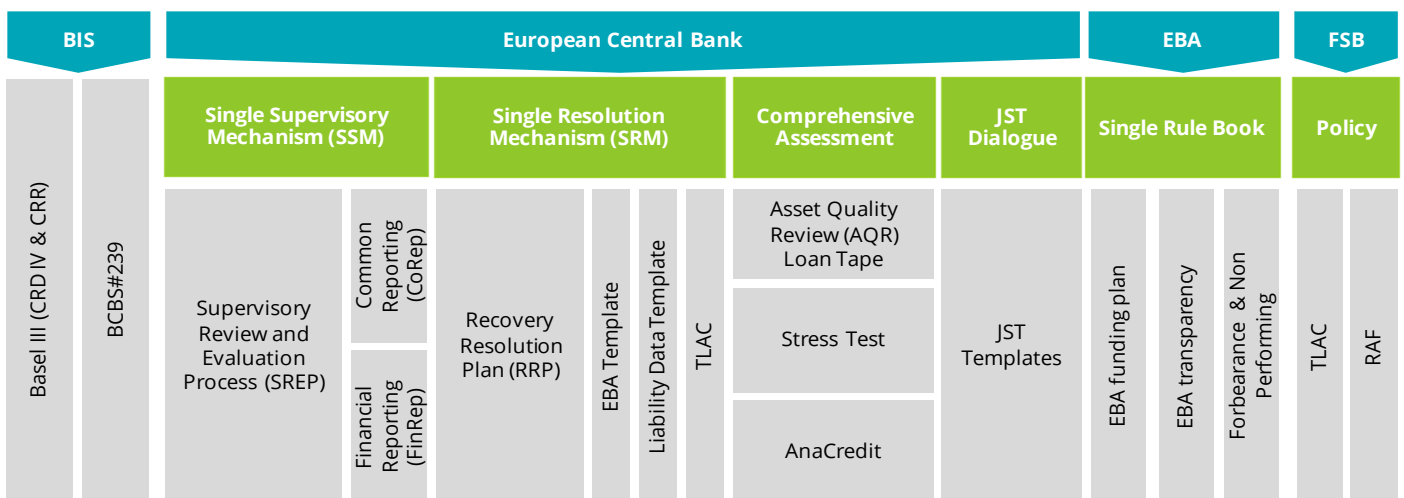
BCBS #239 represents an opportunity for G-SIBs, who must meet further regulatory requirements related to data (like AnaCredit), to homogenize processes and IT architecture.

Likewise, D-SIBs should ideally take advantage of the fact that their implementation plans are at an earlier stage of development to exploit these synergies and economies of scale by

integrating various projects (like the implementation of the AnaCredit ECB template). This should allow for a significant reduction in costs and delivery times.

A recent development that reinforces the importance of strong governance around data quality is represented by the publication of the Targeted Review of Internal Models (TRIM). The main objective of this initiative is to reinforce the controls around the use of internal models and reduce the variance in RWA. The ECB's objective, by publishing this document, is to provide further guidance on emerging regulatory expectations for risk reporting, including quantitative thresholds for each of the core elements of the data quality framework and reporting in the form of a visual report (e.g. using a traffic light (Red/Amber/Green) system).

Figure 8 | REGULATORY PERIMETER



REGULATORY PERIMETER

The analysis on all different regulations represents the starting point for: gathering the required information, identifying the requirements related to the process, detecting the potential overlapping and defining priorities. Therefore, it is crucial to face this challenging environment with a timely and coherent attitude.

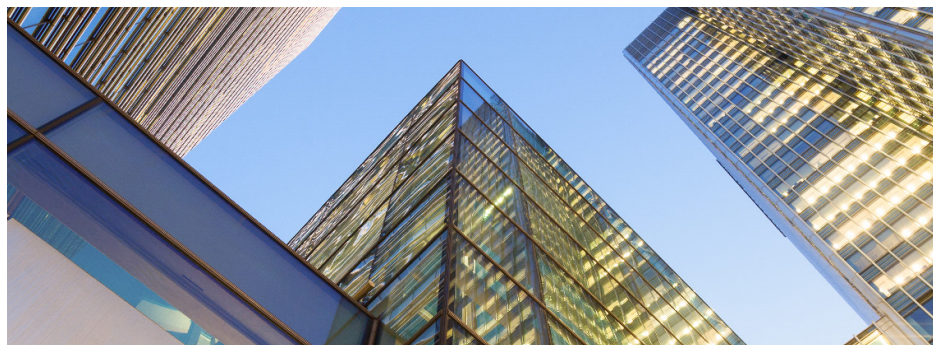
The last mile towards compliance

To date, G-SIBs have achieved significant progress in terms of compliance with BCBS#239, however the target set by the regulation will require further efforts. The Committee has come to the conclusion that **G-SIBs have still several gaps that need to be closed in order to achieve compliance with the principles, a milestone expected by the end of 2018** (with an effective overshoot of 2 years over the regulatory deadline).

From a regulatory perspective a further, non-negotiable, aspect is the ability for banks to demonstrate a consistent level of compliance, both at group and standalone level.

A key lesson learnt regards the planning of a roadmap to compliance and in particular the definition of the Target Operating Model. The best practice approach suggests that the focus should be towards a **forward looking solution**, not solely aimed at the remediation of immediate gaps. The long term approach will result in a better integrated infrastructure leading to a reduction in the impact of manual adjustments and, as a consequence, reduced operational risk. The benefits from this long term strategy will materialise over the years, requiring complete buy-in from senior management and across the whole organisation.

Furthermore, leveraging the insights from the G-SIBs implementation efforts, D-SIBs should include in their plans robust data quality controls geared towards further automation of controls and adjustments. This would, in turn, reduce the need for manual intervention and bring these banks closer to the concept of full compliance as originally intended.



The roadmap should also include a timeline for the closure of compliance gaps, (with specific deliverables) featuring dedicated resources and tangible success metrics (KPI) that demonstrate the implementation progress. The roadmap should take in account:

- Any strategic planning decisions and its implications on the bank's business models and risk profiles, in order to update the working plan and review the project decisions in a coherent manner;
- the bank's in-flight projects, in order to identify common deliverables and exploit potential synergies between different initiatives.

D-SIBs approaching the planning phase should devote specific efforts, according to the regulator, to the self-assessment exercise. This monitoring exercise should aim to underline the initial level of implementation of the BCBS principles, and to identify the gap between the as-is and the to-be situation, as well as root causes.

Ultimately it is possible to identify **three key recommendations valid for each bank planning to initiate or revitalise the journey towards BCBS #239 compliance:**

- **Governance and Process** - Banks must realise how a properly implemented **Chief Data Officer (CDO) function** can be determinant for the effective delivery of a robust data governance process. This is only possible through the allocation of a realistic budget to tackle remediation work and by providing full support from all parties involved in data transformation.
- **IT infrastructure and data aggregation process** - Risk data aggregation requires relevant level of **commitment from banks**, which need to set up **sufficient budget to improve timeliness, accuracy and completeness of the data management framework.** The resilience and robustness of the infrastructure, also under stressed conditions, represents one of the main objectives for the Regulator.
- **Risk Reporting** – Banks must develop their ability to define **robust reconciliation processes within a standardised data quality controls and validation framework.** Robust reporting should allow the required degree of flexibility in order to support the ability for risk managers to analyse and explain data effectively.



Contacts

Coordinators of this publication

Luigi Mastrangelo

Partner
Deloitte Consulting S.r.l.
+39 3480744925
lmastrangelo@deloitte.it

Mattia Monti

Manager
Deloitte Consulting S.r.l.
+39 3403093018
mamonti@deloitte.it

Team Member of this publication

Giuseppe Castellano

Senior Consultant
Deloitte Consulting S.r.l.
+39 3427913056
gcastellano@deloitte.it

Valentina Galasso

Senior Consultant
Deloitte Consulting S.r.l.
+39 3490803304
vgalasso@deloitte.it

Isabella Carannante

Consultant
Deloitte Consulting S.r.l.
+39 3403445366
icarannante@deloitte.it

Contributors

This paper includes contributions and insight by the following financial service professionals from Deloitte Touche Tohmatsu Ltd.

United Kingdom

Enrico Messori

EMEA BCBS 239 Coordinator
Senior Manager
Deloitte LLP
+44 7867156343
emessori@deloitte.co.uk

Germany

Stefanie Kampmann

Partner
Deloitte Consulting
+49 15158004943
stkampmann@deloitte.de

France

Michel Guidoux

Senior Manager
Deloitte ERS
+33 607660568
mguidoux@deloitte.fr

Netherlands

Geert Waardenburg

Director
Deloitte Risk Advisory
+31 620789946
gewaardenburg@deloitte.nl

DTTL Member firms contacts

Austria

Dominik Damm
Partner
Deloitte Financial Advisory
GmbH
+43 1537005400
ddamm@deloitte.at

Greece

Alexandra Kostara
Partner
Deloitte Audit FSI
+30 2106781149
akostara@deloitte.gr

Netherlands

Eelco Schnezler
Director
Deloitte Financial Risk
Management
+31 612345158
eschnezler@deloitte.nl

Spain

Fernando Foncea
Partner
Deloitte Advisory S.L.
+34 932304826
fefoncea@deloitte.es

Belgium

Roeland Baeten
Director
Deloitte Consulting
& Advisory
+32 497233839
rbaeten@deloitte.com

France

Marc Van Caeneghem
EMEA Basel Leader
Partner
Deloitte Conseil
+33 155616588
mvancaeneghem@deloitte.fr

Ireland

Sean Smith
Partner
Deloitte Risk Advisory
+353 14172306
seansmith1@deloitte.ie

Victor Luan

Senior Manager
Deloitte Risk Advisory
+353 14178869
viluan@deloitte.ie

Italy

Antonio Arfè
Partner
Deloitte Consulting S.r.l.
+39 3351350797
aarfe@deloitte.it

Paolo Gianturco

Partner
Deloitte Consulting S.r.l.
+39 3356571811
pgianturco@deloitte.it

Luigi Mastrangelo

Partner
Deloitte Consulting S.r.l.
+39 3480744925
lmastrangelo@deloitte.it

Portugal

Miguel Filipe Morais
Partner
Deloitte FSI
+35 1210422511
mmorais@deloitte.pt

Denmark

Hans Van Leeuwen
Partner
Strategic and Reputation Risk
+45 30936768
hleeuwen@deloitte.dk

Germany

Stefanie Kampmann
Partner
Deloitte Consulting GmbH
+49 15158004943
stkampmann@deloitte.de

Peter Bruhns

Partner
Deloitte Consulting GmbH
+49 1722345787
pbruhns@deloitte.de

Luxembourg

Laurent Berliner
Partner
Deloitte Risk Advisory
+352 621184667
lberliner@deloitte.lu

United Kingdom

Vishal Vedi
EMEA FSI Risk &
Capital Mgmt Leader
Partner
Deloitte LLP
+44 2073036737
vvedi@deloitte.co.uk

Thomas Spellman

Partner
Deloitte LLP
+44 7919545295
thspellman@deloitte.co.uk

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

© 2017 Deloitte Consulting S.r.l.
Graphic Department Deloitte, Italy - SG.072.17