BCBS 239 – Raising the standard

November 2017

pwc

Contents

Introduction

Since it was issued in January, 2013, BCBS 239 (The Basel Committee on Banking Supervision, Principles for effective risk data aggregation and risk reporting) has had profound effects in the banking industry. The BCBS has called out banks and supervisors alike for doing too little to achieve and validate compliance. In the most recent progress update, published by the BCBS in March 2017[1], they noted that only one institution was deemed fully compliant within the three-year deadline.

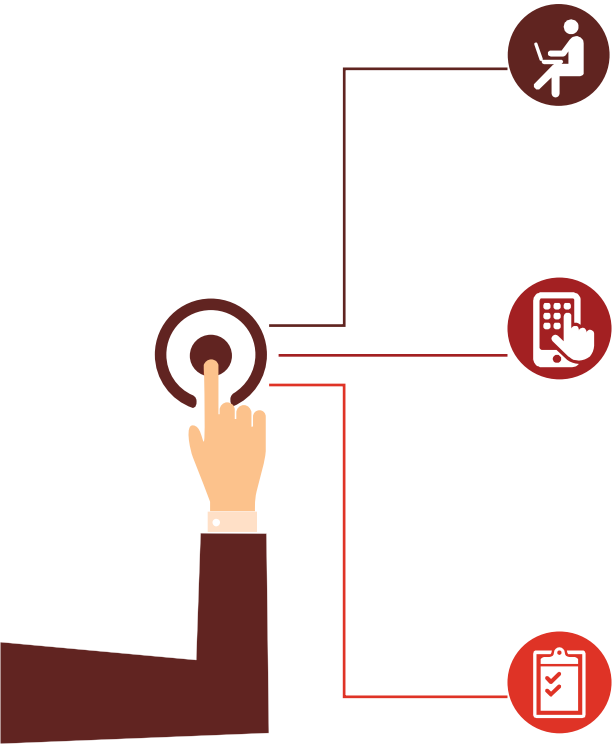
While initially aimed at institutions designated as G-SIBs[2], BCBS 239 has become a de facto standard across the banking industry and several national supervisors are now formally requiring D-SIBs[3] under their jurisdiction to be compliant. In PwC's view, all banking institutions should be considering the principles whether explicitly for regulatory compliance purposes or implicitly for enhancing key aggregation and reporting capabilities. Banks that get closest to the spirit of the principles will be more resilient to future change, better able to respond to threats and opportunities, will face reduced regulatory scrutiny (due to higher confidence), and will have risk functions that play a more strategic role on day-to-day commercial decisions. Risk functions will also work closely alongside Finance, with a common infrastructure and a more integrated service model.

The principles are also garnering attention beyond just the banking sector and provide a benchmark standard for similar requirements across other sectors, such as IFRS17 in the insurance sector. These include fundamental shifts in how data will need to be collected, stored and analysed, which will require enhanced data governance, systems, processes and controls – closely mirroring BCBS 239.

1. Progress in adopting the Principles for effective risk data aggregation and risk reporting - March 2017 (http://www.bis.org/bcbs/publ/d399.pdf). The 4th progress paper published by the BIS.
2. The Financial Stability Board (FSB), in consultation with Basel Committee on Banking Supervision (BCBS) and national authorities, has identified a list of 30 global systemically important banks (G-SIBs), using end-2015 data and the updated assessment methodology published by the BCBS in July 2013.
3. D-SIBs are banks that are assessed to have a significant impact on the stability of the financial system and proper functioning of the broader economy based on a set of assessment methodology similar to that published by the BCBS. In the EU, D-SIBs are termed Other Systemically Important Institutions (O-SIIs)

Based on the March 2017 progress paper banks have cited various reasons for the delays in addressing the principles and among the top challenges are:

- High-level and subjective nature of the principles themselves
- Lack of regulatory guidance on what compliance means coupled with lack of regulatory emphasis (in several jurisdictions)
- The complexity and sheer effort required to overhaul data, systems and underlying architecture, with non-standard data models, conflicting requirements and legacy in-house solutions
- Management fatigue with regulatory-driven programs and investment
- Over-confidence in current capabilities related to risk data aggregation and risk reporting
- Competing demands for a limited budget resulting in the spread of costs and the execution of the BCBS programme across a number of financial years
- Maintaining momentum and alignment across the banking group despite different ambition levels, complexities and supervisory regimes



It has taken the industry and supervisors time to work through these challenges and agree what achieving full compliance means and how to achieve it. For the majority of G-SIBs who are not yet there, the key focus areas are:

Implementation of a Data Management Strategy: Over two-thirds of G-SIBs have appointed group Chief Data Officers since 2013 with an initial focus on establishing data management foundational policies and standards around data governance, data quality, and critical data element management. Many institutions are now in the process of multi-year roll-outs of the foundational policies.

Technology and Architecture Programs: While some banks initiated new programs, most chose to rely on the completion of existing technology programs as part of their compliance strategy. This approach has proven challenging due to the difficulty of managing inter-dependencies and the complexity of the programs themselves. Most institutions still have much to do in this area and we see notable differences in interpretation of what's required amongst supervisors on this topic.

Addressing end-to-end Control weaknesses: Whilst most banks have developed control frameworks and policies to address controls across the data life cycle from origination through reporting, institutions are still struggling to implement and operationalise controls across the end-to-end data and reporting architecture. Key challenges include data quality controls, control and remediation of end-user-computing (EUC) applications, and reconciliation controls related to risk and finance data alignment.

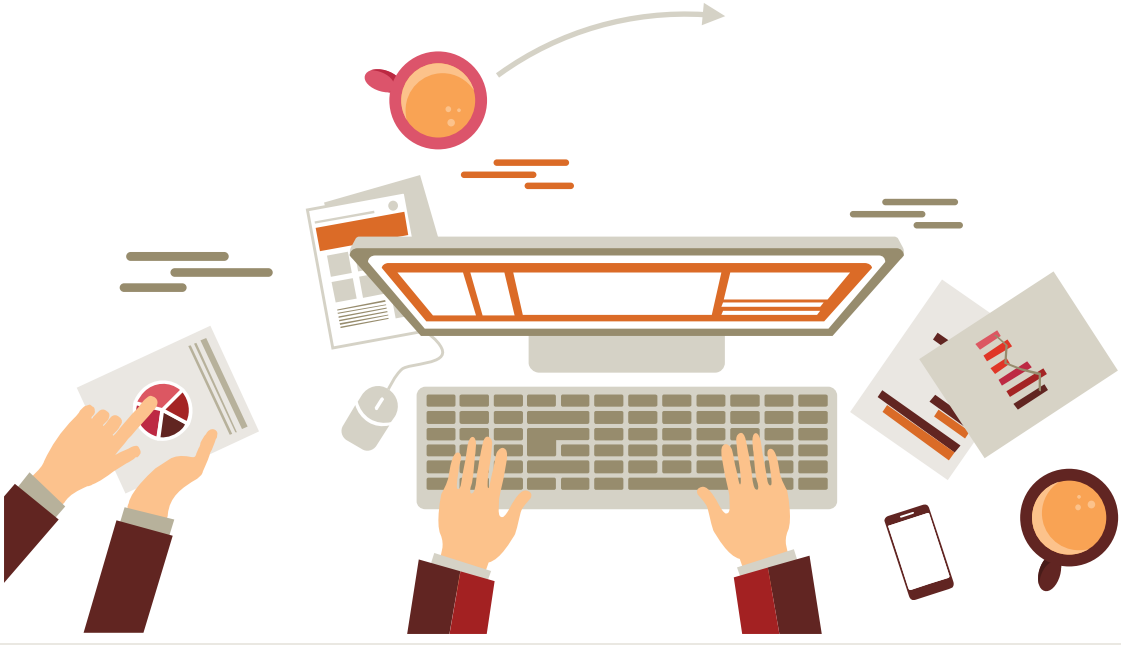
In this report we provide PwC's overall perspectives on how institutions are approaching BCBS 239 to address these challenges, where supervisors stand in various jurisdictions, and key considerations for moving forward.

Compliance approach and current situation

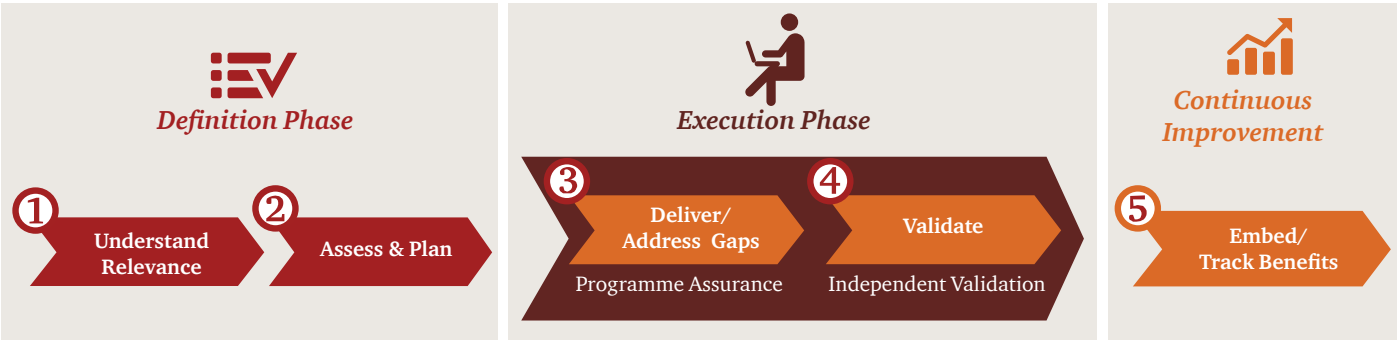
Overall approach and situation

Well into year five of the BCBS 239 journey, it has been universally recognised that achievement of a 'compliance milestone' is not an appropriate goal. Rather, banks have realised that deployment of the key capabilities required to address the objectives of BCBS 239 will require a continuous effort. Institutions have followed an approach comprising three phases:

1. ***Definition:*** In this phase, banks have worked to understand and interpret BCBS 239 through reviewing principles, determining a definition of compliance, determining an approach for assessing the current level of compliance along with gaps and then agreeing to an execution plan and scope with their supervisors.
2. ***Execution:*** During this phase banks have executed programs and initiatives to address key gaps and enhance capabilities across data management, risk data aggregation and reporting standards and processes, governance and control frameworks, and technology infrastructure and architecture. Beyond just addressing any gaps identified, the ongoing "fully compliant" business-as-usual operating model is defined such that BCBS 239 programs transition into ongoing activity. Banks also establish and operate independent validation functions as required by BCBS 239 in order to assess progress toward goals. While this phase is generally focused to achieve key objectives by a regulatory deadline, it does not represent the end of the journey.
3. ***Continuous Improvement:*** In this phase, institutions continue to increase both the level of maturity of capabilities deployed as well as the scope of application of those capabilities. BCBS 239 disciplines are embedded in business as usual operating models and the "return on investment" in BCBS 239 capabilities is measured.



The diagram below represents the key steps in these phases and provides a view of where various types of banks are in the journey:



Banks are at different stages in the journey, depending on their type and maturity

Where are banks in the journey?				
• Potential D-SIBs • Tier2, 3 Banks	• Recently designated D-SIBs and G-SIBs	• G-SIBs past deadlines but not fully compliants • D-SIBs either ahead of or past compliance deadlines	• All banks past compliance deadlines (G-SIB and D-SIB) • Banks with upcoming compliance deadlins (D-SIBs)	• All banks past compliance deadlines (G-SIB and D-SIB)

Generally, G-SIBs remain in the execution phase and are working to complete longer term programs and address key gaps found during internal validation exercises as well as regulatory exams.

Beyond this group of banks, some supervisors have formally adopted BCBS 239 as a requirement for the largest banks under their supervision including Canada, Singapore, and Hong Kong. Regardless of formal supervisory action, PwC believes all institutions should be developing strategies for the incorporation of the BCBS 239 principles.

While national regulators (or "supervisors" as they are termed in the BCBS 239 Paper) have not converged on a specific mechanism for measuring compliance, the original "stock-taking questionnaire" released in March 2013 remains a "guidepost" for assessing compliance. Many banks did their initial assessments and gap remediation planning on the basis of this questionnaire and later found that due to the highly interpretive nature of the questions, specific outcomes and associated action plans were difficult to define.

To address these challenges, PwC has worked with various banks to assist them in adopting an approach which focuses on translating the BCBS principles and their associated requirements into a set of specific business capabilities which must be demonstrated. This approach has enabled banks to define specific and measurable business outcomes along with associated artefacts that need to be achieved. In turn, this enables targeted and specific action plans to be developed.

The capability model at the core of this approach allocates key capabilities into four key pillars:

1. Data Management
2. Risk Standards and Processes
3. Governance and Control
4. Technology Infrastructure and Architecture

An overview of the model is shown below

- Enterprise-wide standards, processes & tools for data definition, data ownership, & identification & adoption of golden sources
- Consistent data models/ hierarchies across front office, risk & finance
- Adopted reference data standards including single identifiers (e.g., LEI)
- Data quality framework for measurement, monitoring & reporting
- Remediation of existing data quality issues e.g., adjustments, overrides, fallbacks & breaks

- Documentation & implementation of risk data aggregation and risk reporting standards, including board & senior management approval
- Identification, mitigation & remediation of limitations in risk aggregation & reporting capabilities
- Identification of critical data elements (CDEs)
- Specification of risk information requirements (timeliness, accuracy, etc.) including for ad-hoc requests & stress/crisis period reporting
- Standardisation of risk MI used in governance committees
- Standardisation of risk aggregation methodologies
- Integrated exception reporting and validation checks

- Governance, policies & controls to enforce:
  - 1st line of ownership & quality of data
  - Production of risk data within defined aggregation & reporting standards
  - Enhanced standards for end user computing
- Reconciliation of data to source systems
- Reconciliation between risk & accounting data
- Robust control framework for risk data (equivalent standard to accounting data)
- Certification processes for data, aggregation processes & risk reports
- Implementation of escalation channels & remediation mechanisms
- Board & senior management involvement
- Independent validation process

- Group-wide IT strategy & bank-wide data architecture roadmap to meet BCBS 239 capabilities
- Group-wide master data management
- Adoption of common reference data across risk & finance; systems & feeds updated
- Elimination of reliance on manual aggregation & reporting methods & end user computing
- Automation of controls over timeliness, completeness & accuracy of data
- Flexible aggregation & reporting capabilities to meet ad-hoc reporting requirements & drill-down into supporting granular information
- Ability to quickly aggregate & report critical risk information during stress/crisis periods

4 pillar BCBS 239 capability framework

This capability-based approach includes direct mapping back to the principles and paragraphs and has been adopted by many of our clients in various regulatory jurisdictions. It has proven to be an effective way to define specific and measurable outcomes for BCBS 239 compliance.

Regulatory perspectives

Like the banks, supervisors have also been on a journey in understanding the scale and complexity of implementing the BCBS 239 principles. The original three year compliance timeline was thought to be sufficient for most banks, and it was understood that many were already running transformational change initiatives that would deliver the building blocks of compliance. However, many of these programmes failed to deliver, and it became clear that full compliance would require a significant multi-year effort beyond three years.

The nature of BCBS 239 is subject to interpretation as it is aimed at banks of all kinds (although initially focused on G-SIBs and D-SIBs, supervisors are following the recommendation to apply it to a wider range of banks). In the absence of any clear guidance or standards from supervisors on what would be "good enough", language in the industry changed to only achieving 'material compliance' by the 1st January 2016 deadline for G-SIBs, with "full compliance" due at a later date. For "material compliance", banks prioritised their most significant risk types, subsidiaries and typically focused only on group risk board reporting. Smaller and midsized banks such as D-SIBs also seem to be following this approach.

Supervisors were initially sceptical on this approach, and sought to understand why banks were delaying the full implementation of the principles. But, in light of the large-scale changes that most banks were planning, they acknowledged the need for banks to prioritise the most important areas first and take a proportional approach. In 2015 supervisors stated that banks should ensure that boards were aware of and had approved the approach to compliance, and that materiality could be justified in the context of risk appetite, geographic footprint, business structure and strategy[3]. More recently supervisors have challenged banks to ensure risk reporting is also covered for their material entities, and the focus is no longer just prudential risks but also non-financial risks (e.g. operational and conduct risk).

3. Initially supervisors provided this guidance in letters sent directly to the banks themselves, but it was also described in section 6.3 of the December 2015 BCBS progress paper: http://www.bis.org/bcbs/publ/d348.htm

An additional requirement that has emerged has been the expectation that banks should also apply BCBS 239 to their external financial and regulatory reporting. Although the focus of the principles is on *internal* risk reporting, as early as 2014 some supervisors indicated that they would review regulatory and stress testing returns as an input on their decision as to whether banks are compliant. More recently the ECB has gone further in explicitly stating that banks should include financial and regulatory reports as in-scope. Although this is a logical step, and much of the data is common, typically processes, systems and specific definitions used for external reporting are different; so the impact of bringing them into scope is a significant increase in work. A repeated area of concern has been higher reported levels of compliance for Principles 7-11 (risk reporting) than for Principles 3-6 (data aggregation). More critically, principles 1 and 2 (governance and data architecture and infrastructure) are seen as pre-conditions to compliance and yet are consistently lower rated than others.

In early 2016, national supervisors defined a range of different approaches to assessing compliance, as summarised in table 3.1. However despite continued requests from the industry for greater clarity on where the bar is being set, supervisors have remained reticent to provide specific guidelines or minimum standards. They have instead emphasised that there is not a one-size-fits-all approach for BCBS 239, and that each bank will be different. However, arguably this has exacerbated the challenges of compliance and the significant "interpretation risk" that banks face (the risk of being called non-compliant at a later date due to a difference of opinion on interpretation with the supervisor).

Table 3.1: Supervisory approaches to assessing compliance with BCBS 239

Territory/ Supervisor	Approach
EU ECB	• The ECB has been amongst the most active of supervisory authorities on BCBS 239, naming it as one of their Single Supervisory Mechanism (SSM) priorities for 2016 and 2017. • Conducted a thematic review on BCBS 239, focusing on 26 major banks in the European banking sector: – Focused on deep dive reviews of Tier 1 banks and issued a detailed questionnaire to Tier 2 banks in Q2 2016, followed up with detailed meetings and on the ground reviews in late 2016 or early 2017. – Ran a fire drill exercise on Credit and Liquidity Risk metrics, requiring responses within 48 hours including information on data lineage and controls. • In Q2 2017, the ECB issued letters to banks summarising the outcome of the thematic review, with two key messages: – Banks are expected to include external and regulatory reporting in the scope of BCBS 239, and – More progress is expected on enhancements to systems and data architecture. • Further scrutiny of compliance is expected, explicitly for BCBS 239 and as part of other related ECB activities such as the Asset Quality Review (AQR) and Targeted Review of Internal Models (TRIM) exercises.
UK PRA	• Conducting a rolling 3-year assessment process, based on detailed compliance validation reviews of a tranche of principles per year carried out by bank Internal Audit (IA) functions. • In February 2016 bank accountable executives were required to provide an overall summary of their compliance status across all 11 principles. Then by end-June IA functions had to provide review findings on the first tranche of principles (1, 2, 3 and 7). • In 2017 accountable executives were required to provide an updated view, followed by IA reviews on the second tranche of principles (4, 6, 8 and 11), in addition to and update on progress against the first tranche from 2016.

Territory/ Supervisor	Approach
	• Have allowed banks to adjust the timing and scope of these reviews individually based on their own programme dates and variations in approaches. • The PRA have provided limited feedback to banks on the reviews themselves, although did request that IA functions report their findings back at a paragraph level, by risk type.
US Fed and OCC	• The Fed has generally taken a more "hands-off" approach to BCBS 239 due to their reliance on the annual CCAR Stress Testing process as the mechanism for reviewing banks' risk data aggregation and reporting capabilities including control environments. • For compliance monitoring the Fed has largely relied on bank Internal Audit and Independent Validation functions of the banks to provide judgement on compliance levels. • The OCC has developed 'heightened standards' for banks under their supervision with assets greater than $50 billion and these standards refer to BCBS 239 as the guiding set of principles for risk data aggregation. • The OCC has undertaken a number of programme reviews, and has requested that some banks take specific remedial actions within a defined time frame.
Asia CBRC and JFSA	• The JFSA has generally taken a "hands-on" approach to compliance conducting frequent follow-up discussions with Banks during the compliance journey. The JFSA planned to finalise compliance assessment by July 2016, requiring Banks to compile a final self-assessment survey, conducting interviews with C-suites and Internal Auditors and fire-drilling on data aggregation and reporting capabilities introducing stress testing scenarios. It is now following up on G-SIBs status towards full compliance with BCBS239 by periodic interviews. • The JFSA nominated 4 banks as D-SIBs in December 2015 and is requiring them to comply with BCBS 239 by December 2018. • The compliance deadline for Hong Kong is 1 April 2018. However, we have noted that some of the 5 designated D-SIB banks have just started on their gaps assessment. It is very likely that similar to the experience of the G-SIBs, they will not achieve material compliance by the deadline and would require another 2-3 years down the road. • Whilst China did not officially adopt BCBS 239, on 12 September 2014, the CBRC issued a "Guidelines on Internal Control of Commercial Banks" whose articles are largely similar to the principles adopted in BCBS 239. Some key differences exist : (i) that the guidelines are applicable to all financial institutions, asset management companies, trust and leasing companies and not just the systematically important ones (ii) that the guidelines extend beyond the 11 Principles highlighted in BCBS 239 and also includes provisions for HR policies on professional ethics and to set up professional ethics and capabilities as important selection and recruitment criteria and performance appraisals. (iii) it takes immediate effect from the date of issuance (iv) it spells out the supervisory measures than can be taken against violations of the guidelines, and non-timely remediation • The Singapore MAS has still been relatively light in terms of its supervision over the DSIBs' programmes. There is an intention to tighten their review via modular checks on a periodic basis up to the end of the compliance deadline for the Singapore DSIBs, which is 2019. • The other supervisors in Southeast Asia are still taking a wait-and-see approach. However, certain aspects of the BCBS 239 framework, e.g. data quality have been embedded into their existing regulatory framework to make the adoption a less painful process in due course.
Switzerland FINMA	• FINMA have required banks to engage external audit firms for detailed reviews, and have applied a more stringent and purist interpretation of what is required for compliance.

By the end of 2016, most G-SIBs had met their own internally defined material compliance standard, albeit with an agreed book of remediation work to address specific findings from internal audit or supervisory reviews. However, of greater concern to banks has been determining how best to define 'full compliance' (see Figure 3.2 on defining compliance). Then, once that standard has been met, how to ensure that the next issue doesn't automatically revert that status back to non-compliance. Supervisors have shown pragmatism in acknowledging that banks will likely have further work to do after full compliance, as part of a process of continuous improvement or the delivery of longer-term strategic change. But this remains a hot topic, and one where clearer standards will be needed as supervisors start to apply punitive measures and require specific remedial activities. Banks will also want to ensure that there is a level playing field.

Table 3.2: The challenges with BCBS 239

Simply landing on a common language for compliance has proven difficult for banks

Term	Definition approaches
Largely complied with	• Language from the Basel Committee stock-taking questionnaire, commonly adopted as the standard ratings system for the principles • Aligned to a '3' rating and defined as "*only minor actions are needed in order to fully comply with the Principle/requirement*"
Material compliance	• Typically used interchangeably with "Largely complied with", although most banks have also applied it across a prioritised sub-set of their full compliance scope
Fully complied with	• Terminology used in the Basel ratings for a '4' rating, defined as "*the objective of the Principle/ requirement is fully achieved with the existing architecture and processes*" • Has led to significant debate within banks, as there is no commonly agreed compliance benchmark and it is not practical to achieve 100% compliance
Compliance	• Due to the absolute level implied by "full" compliance, some banks have dropped this term and refer instead simply to achieving compliance, or in some cases adherence with the principles • Whilst understandable in concept, banks are likely to remain tied to the Basel ratings system by supervisors for the time being
Continuous	• An interpretation that compliance means banks can evidence that issues are addressed in a timely manner, and scope be extended to lower levels of the organisation, as part of business as usual as opposed to a formal change programme • An emerging theme within some European banks has been the extent to which tactical short-term solutions can be put in place for full compliance, ahead of longer-term strategic ones • Many banks have transformational IT programmes beyond the time horizon of their BCBS 239 deadlines, and are pushing the concept of continuous improvement for these enhancements rather than expecting everything to be done before full compliance is declared

The March 2017 progress paper published by the Basel Committee provided an update on G-SIB's level of compliance. For the first time results were based on data captured from national supervisors in 2016 and not from a self-evaluation conducted by the banks as seen in the previous progress reports. Another notable change was that the paper provided specific examples of good practices of largely and fully compliant banks as well as ineffective practices. Supervisors have been clear that these aren't minimum standards for compliance, but they do provide greater clarity on what is seen as "good enough". At a minimum, banks should have reviewed their approach against these practices and satisfied themselves that they have a clear rationale for any gaps.

In summary, PwC still sees inconsistency across supervisors on the application of the principles, although the March 2017 progress update and more recent specific guidance to individual banks has begun to clarify expectations. The Basel Committee working group on BCBS 239 – formerly the Working Group of SIB supervision, now named the Risk Data Network – is enabling greater cooperation amongst supervisors, but further guidance is likely to be developed and issued by local supervisors. PwC expects specific expectations to continue to be discussed bilaterally between banks and their supervisors, as regulators continue to refrain from setting a precedent that may be constraining and stipulative for D-SIBs and smaller organisations.

Key takeaways

Based on the current state of compliance with BCBS 239 across the industry, and the most recent progress update paper from March 2017, there are 8 key take-aways for banks to consider:

1. *Defining the thresholds for Full Compliance is an imperative*

All institutions subject to the Principles should ensure they have **clear definitions of full compliance, with tangible measures.** Banks must also define their own **criteria and minimum standards** for remaining fully compliant. In successful projects transparent documentation of decisions that have been through appropriate governance with clear rationale is key.

2. *D-SIBs and smaller banks are strongly encouraged to start implementation early*

Banks that are working towards a compliance deadline should **increase their level of communication with their supervisors with respect to their scope and plans** in order to avert surprises. Institutions who are not yet formally subject to BCBS 239 should **consider undertaking initial assessments** as the Principles are becoming the de facto gold standard for data aggregation and reporting and overlap with multiple other regulatory expectations.

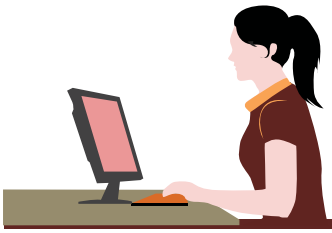
3. *Banks must do better around clarity and rationale for compliance scope, including regulatory reporting*

Banks should prepare a **formal scoping document, indicating detailed rationale** for inclusion/exclusion across the key dimensions of line of business, legal entity, and risk area, key reports, and critical data elements. Supervisors have also called out **application of the Principles to Regulatory and Financial reporting** as an effective practice demonstrated by leading institutions.

4. *Clear progress needs to be made towards a strategic risk architecture for full compliance*

Banks don't need to have completed their strategic target architecture implementation for full compliance, instead supervisors expect **significant progress** to have been made, for example explicit rationalisation of end user computing solutions, process automation and golden sources for key reference data dimensions, and evidence of **ongoing investment in enterprise-wide architecture and infrastructure.**

5. *Forward-looking, ad-hoc and dynamic capabilities highlighted with greater emphasis*



Some clarity on expectations around reporting capabilities is emerging and the focus is on **more forward-looking, ad-hoc, and dynamic capabilities** with supporting policy/procedures for ad hoc/stress crisis reporting. To meet expectations, banks are adopting reliable and agile technological solutions such as real-time dynamic dashboards and digitalization of risk reporting in general.

6. *The Principles need to be embedded, with clear ownership, throughout the Enterprise*

Top of the house compliance is not good enough – assessments and data remediation should be done **across all business units and material geographies.** Business ownership, for example of data controls and data remediation is also key – responsibility for compliance must be **broader than just Risk. On top of that supervisors expect senior management to actively communicate and sponsor BCBS 239 in their banks.**

7. *Leverage industry standards rather than create your own*

Industry taxonomy standards such as the Legal Entity Identifier (LEI) are specifically called out as good practice and banks are encouraged to adopt them – in addition to LEI we see industry momentum around the FIBO (Financial Instrument Business Ontology) standard as well.

8. *Root-causes analysis is encouraged where Banks further delay compliance*

Banks will need a **detailed explanation of why they have not been able to comply in a timely manner.** They are encouraged to conduct **root cause analysis regarding delays** in implementation and have a realistic plan in place on how to overcome possible operational obstacles such as lack of resources.

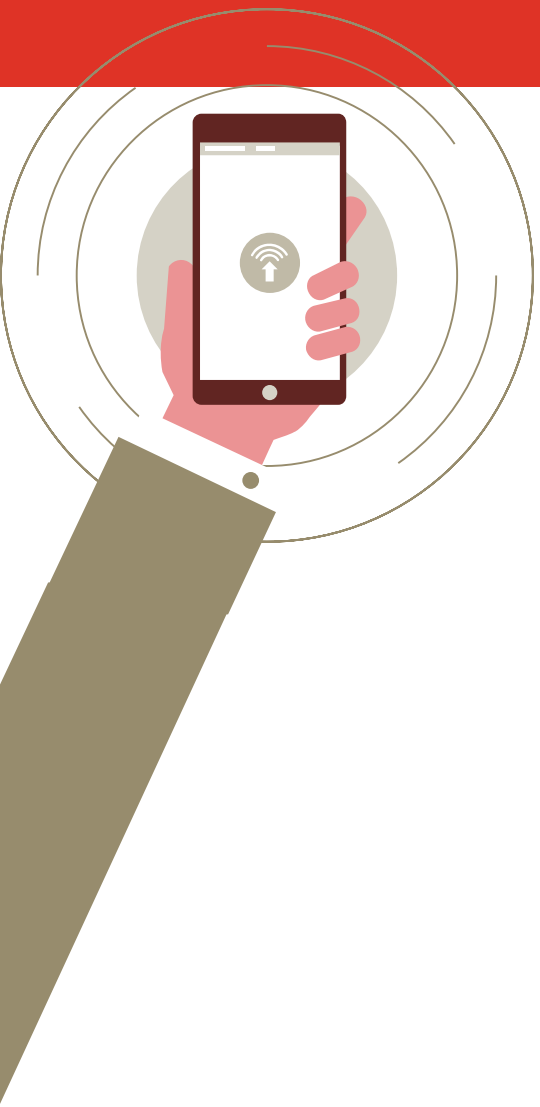
Conclusion

The BCBS 239 Principles have become the de facto standard across the banking industry and are profoundly changing the way that banks think about their risk data, systems and controls. Defining what it means to be "fully compliant" and then moving towards that target is not straightforward and requires multi-year programmes of work. On the other hand, some banks are using BCBS 239 as a platform for building competitive advantage and efficiency. Key investment areas include process digitisation, a rigorous redesign of their IT architecture and broad commitment for new levels of data throughout the bank, not only in risk, finance and regulatory domains but also for client and sales data.

G-SIBs should have made significant progress towards compliance but have lots more to do. The bar is rising and doing "just-enough" is no longer an option. Key success factors include an engaged and fully informed board, strong senior executive sponsorship, a clear compliance plan based on business outcomes, and regular evidence that demonstrable progress is being made.

D-SIBs and banks at earlier stages in their compliance programmes must learn from the pitfalls larger banks have faced, but be aware: it's harder than expected. It's not just another regulatory hurdle, it requires a step-change in capabilities, mindsets and culture. If banks are not yet subject to BCBS239, they should act like they are.

Contacts



Jonathan Riva

Partner
PwC Canada
+1-416-815-5069
jonathan.riva@ca.pwc.com

David Yakowitz

Managing Director
PwC US
+1-630-640-5071
david.yakowitz@us.pwc.com

Irene L Liu

Partner
PwC Singapore
+65-6236-4098
irene.l.liu@sg.pwc.com

Jun Muranaga

Partner
PwC Japan
+81-80-1347-2227
jun.muranaga@jp.pwc.com

Sami Khiari

Partner
PwC Germany
+49-30-2636-1453
sami.khiari@de.pwc.com

Tom Fish

Director
PwC UK
+44 207 2126341
tom.f.fish@uk.pwc.com