

# *Talking about compliance:* BCBS 239 implementation in South Africa

*South African BCBS 239  
Survey*

May 2016





# Table of Contents

<i>Acknowledgements</i>	4
<i>Executive summary</i>	4
<i>Background to BCBS 239</i>	6
<i>BCBS 239: A global perspective</i>	7
<i>Overview of the survey</i>	8
<i>Detailed survey questions and responses</i>	9
<i>Appendix 1: Survey questionnaire</i>	32
<i>Appendix 2: Summary of the BCBS 239 principles</i>	36



## **Acknowledgements**

We would like to take this opportunity to thank each of the banks that participated in the survey. Your time, informative discussions and open communication contributed to the success of the survey and provided us with valuable feedback.

## **Executive summary**

South African banks, like their global counterparts, continue to face significant challenges with their programmes for the implementation of the Basel Committee on Banking Supervision's Principles for Effective Risk Data Aggregation and Risk Reporting (BCBS 239). The industry recognises the importance of the Principles as not only a compliance imperative but also a strategic enabler. Across all the banks we interviewed, the project has received support at both executive management and board level. Significant amounts of time and money has been invested and will continue to be invested in this programme. SA banks recognise that compliance will deliver a more robust, sustainable and responsive risk management capability. The banks are focusing on doing things right, and most of the programmes they have initiated to support risk data aggregation and risk reporting (RDARR) compliance are expected to extend beyond the 1 January 2017 SARB deadline.

The survey highlighted several themes across South African banks. These are summarised below.

### **Key messages**

#### **Most banks are on track to meet SARB deadline**

**A**

Most banks expect to meet the deadline set by the South African Reserve Bank (SARB), although there is no single definition of compliance. The shape and form of what the banks define as compliance now and in January 2017 varies from bank to bank – which is not unexpected, given that BCBS 239 is principle-based.

#### **Change needs to be considered holistically**

**B**

The practical integration/alignment of BCBS 239 with other strategic and regulatory initiatives (e.g. IFRS 9, cyber security etc.) remains challenging. Judging from our interviews with respondents, all of them recognise that there are overlaps and potential efficiencies to be gained from a more holistic approach. However, it was not clear how the banks are ensuring, practically, that decisions being taken under the RDARR programme do not conflict with or duplicate work being done elsewhere in the bank.

#### **Approach to data seems to be led by Business and is not Bank wide**

**C**

Most of the large South African banks have adopted a federated model for their BCBS 239 programmes. Under this model, implementation of the programme is driven by the business units themselves. Small central teams act as subject matter experts, setting frameworks and standards while providing oversight to ensure that the overall programme remains on track. BCBS 239 requires that banks are able to provide the group board with an aggregate view of the organisation's risk profile relative to its risk appetite (not a single metric, but split by risk types and defined appetite metrics/limits). SA banks should consider whether the siloed or business unit level form of reporting will enable them to fully meet the Principles, i.e. give them the ability to properly aggregate data up to group/ bank level.

### ***The cost of BCBS 239 is expected to be significant - likely in excess of R100m***

D

Though the level of investment that banks are making on BCBS 239 is hard to measure, all agree that it is significant. A number of respondents noted that it was difficult to isolate spending on RDARR, as they do not view it in isolation. Most of them are making significant investments in systems and data that have a business and strategic focus. As part of this investment, they are ensuring that the requirements of BCBS 239 are addressed. Those that were able to isolate the cost indicated that it was projected to be in excess of R100 million. However, the amounts SA banks expect to spend seem to be low compared to their international counterparts, even when their relative sizes are taken into account. Local banks should therefore consider whether they have perhaps underestimated this cost.

### ***Majority of operations outside of SA have been scoped out of initial coverage***

E

Most non-bank and foreign operations have been removed from scope at this stage. All of the respondents have focused on operations that would provide them with the highest level of Risk Weighted Assets (RWA) coverage. As a result, non-bank operations and non-material Rest of Africa (RoA) subsidiaries, where applicable, have been excluded from the initial phase of the programme. The expectation is that these will be brought into scope after January 2017.

### ***Skills deficits pose serious challenges to BCBS 239 programmes***

F

A lack of sufficient IT, data and programme management skills and deficiencies in current IT systems and data infrastructure represent the biggest challenges faced by local banks in implementing their BCBS 239 programmes.

### ***Significant divergence in the number of metrics chosen***

G

The number of metrics and underlying data elements varies significantly from one bank to the next, ranging from 16 metrics at one level to 150 metrics at the other end of the spectrum. The average number of metrics noted was 80-100. Although the smaller banks tend to have fewer metrics when compared to their larger counterparts, the size of the bank was not necessarily a clear driver for this disparity. There has also been some disparity in the number of metrics in scope for the larger banks. The main driver is the definition of what a key metric is – something that is subjective and depends on the needs of the specific bank.

### ***Most banks have not established formal data governance organisations***

H

Unlike their international counterparts, most of the SA banks have not appointed or created a dedicated chief data officer (CDO) or data office. Data is mainly managed at a business level, with a senior data officer's role and functions being fulfilled by designated persons at this level. Effective data governance will soon be a source of competitive advantage, and banks need to make sure that this area receives appropriate attention and resources.

### ***Immature finance and risk alignment***

I

Most of the banks indicated that their risk and finance alignment is limited, however these banks have medium term targets to align such processes. Major challenges cited by the respondents across the three alignment areas included multiple sources of both risk and finance data, independence and a silo approach stemming from the fact that most risk and finance functions have evolved separately, legacy systems (both in risk and finance, both of which have historically operated independently of one another) and data reconciliation difficulties.

### ***A robust approach to BCBS 239 compliance certification is required***

J

Some banks are leaving it up to their internal audit teams to determine how to assess compliance against the Principles. In our view BCBS 239 programmes need to play a part in defining an approach to certifying or confirming compliance status, thus linking all of the activities and deliverables back to improvements against the principles. This is a complex process.

### ***Target compliance state needs to be defined with full compliance in mind***

K

Most SA banks are planning to achieve material compliance by 1 January 2017. However, most of the banks interviewed had not yet defined what full material compliance means for their organizations. The banks thus run the risk of missing their target if they are not considering material compliance in the context of full compliance.

### ***SA banks may be challenged on their scope***

L

Given that SA banks are smaller and simpler when compared to GSIBs (Global systemically important bank), SA banks need to ask themselves whether there is a risk that the regulator might have higher expectations on compliance based on lessons they have learned from their international counterparts.



## **Background to BCBS 239**

One of the lessons learned from the global financial crisis was that banks' information technology (IT) and data architectures were inadequate to support the broad management of financial risks. Many banks lacked the ability to aggregate risk exposures and identify concentrations quickly and accurately at the bank group level, across business lines and between legal entities. Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices. This had severe consequences for the banks themselves and for the stability of the financial system as a whole. As a result, the Basel Committee on Banking Supervision (BCBS) issued the Principles for Effective Risk Data Aggregation and Risk Reporting in 2013, colloquially known by the paper's reference number, BCBS 239. The paper presents a set of 14 Principles aimed at strengthening banks' risk data aggregation capabilities and risk reporting practices. Overall, the Principles set out in BCBS 239 require banks to assess and evidence their risk data and reporting capabilities and to establish ongoing governance, monitoring and assurance.

BCBS 239 aims to achieve the following objectives:

***1. Enhance the infrastructure for reporting key information so as to support the board and senior management in identifying, monitoring and managing risks.***

***2. Improve the speed at which information is made available and shorten the decision-making process throughout the banking organisation.***

***3. Enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures at the global consolidated level.***

***4. Reduce the probability and severity of losses resulting from risk management weaknesses.***

***5. Improve the organisation's quality of strategic planning and its ability to manage the risk of new products and services.***



## **BCBS 239: A global perspective**

Generally, the industry underestimated the scale of the challenge posed by complying with the Principles. The positive is that institutions have pushed the ‘do it right’ rather than ‘do it quickly’ message to regulators regarding initial vs longer-term compliance. Global Systemically Important Banks (G-SIBs) have encountered, and continue to experience, a number of issues and challenges in delivering their BCBS 239 programmes.

We summarise some of these below:



### **A. Increased interest from the regulators**

- The Basel Committee is increasingly pressuring supervisors to take a more active interest in enforcement of the Principles as required by Principle 12.
- The Prudential Regulation Authority (PRA) and European Central Bank (ECB) have informed banks that they will use regulatory and stress testing returns as an input on their decisions of whether banks are compliant. They have indicated that if returns are late or inaccurate they will view those banks as non-compliant.
- The PRA has been the most prescriptive about how they will assess compliance. They will do this on a rolling plan basis, selecting a tranche of principles for assessment each year.
- The PRA has indicated that they will rely on internal audit reviews of compliance. The ECB in contrast are putting large assessment teams in place in Frankfurt and seem more intent in visiting back and conducting assessments later in 2016.



### **B. Level of compliance vary by region and by bank**

- UK/EU banks have reported that they’ve made less progress on the Principles than US and other global banks, but there is a question whether the UK/EU banks have simply been more realistic with the main areas of challenge; those being infrastructure and data accuracy, integrity and adaptability.
- UK G-SIBs are working towards material compliance as they’ve defined it. Most banks have uncovered issues for which they will need to put in place compensating controls or tactical fixes in order to meet the compliance deadline.
- Some European banks have realised they need to more fundamentally re-think their programmes and push back their expected compliance dates.



### **C. Still no definitive view on “what compliance means”**

In the absence of specific compliance criteria, the industry has moved to a “capabilities-based” view of compliance. Institutions are agreeing which capabilities must be demonstrated and at what level of maturity with their regulators which will provide a basis for examination of compliance.

- Institutions are pushing the ‘do it right’ rather than ‘do it quickly’ message.
- There is still a lack of clear guidance from supervisors on what they consider compliance to look like, but some isolated examples of standards are being shared by, for example, the Canadian regulator.





#### **D. Significant work will need to be done to achieve full compliance**

- The compliance deadline for G-SIBs has now passed, but most banks still have a significant amount of work to do before they will achieve full compliance. Key areas where significant work remains to be done include full data lineage back to source, common reference data, integrated taxonomies between risk/finance, and independent validation.



#### **E. Embedding BCBS 239 into the business remains a challenge**

- Most banks have struggled to push BCBS 239 compliance into the business, as it tends to be seen as a risk problem or ‘just a data programme’. Full compliance requires a more fundamental culture shift from the reactive to proactive use of risk information. More fundamentally, the business needs to take ownership of ongoing compliance with BCBS 239.

### ***Overview of the survey***

Following the publication of BCBS 239 and its adoption by the SARB as confirmed in directive D2/2015, PwC were keen to ascertain how much progress local banks had made with their own compliance journey. Specifically, we wanted to understand the following:

- a. Are South African banks, eligible institutions and branches of foreign banks on track to meet the SARB deadline of 1st January 2017?
- b. What are the key challenges that banks are experiencing on their BCBS 239 journey, and are there any challenges unique to the South African industry?
- c. What level of importance is being placed on achieving compliance with BCBS 239?
- d. What key decisions have been taken by banks as part of their implementation, and how do these compare to those of their international counterparts, e.g.
  - Scope dimensions and definitions
  - Breadth of metric coverage
  - Definition of success
- e. How well integrated (if at all) is the BCBS 239 project with other strategic and regulatory initiatives being conducted by the banks?
- f. How are local banks defining BCBS 239 success?

To obtain an understanding of these issues, we conducted a survey in which banks were requested to respond to a set of questions (refer to Appendix 1 for the full questionnaire). After the surveys had been completed, we held an interview session with each of the respondents to get a better understanding of their responses. The survey, which was conducted in March 2016, covered eight major banks in South Africa.

In the pages that follow we look at each of the responses by SA banks to the survey.

What was interesting to note, was that two banks had voluntarily accepted elected to comply with the BCBS 239 Principles, even though there was no explicit regulatory requirement placed on them to do so.



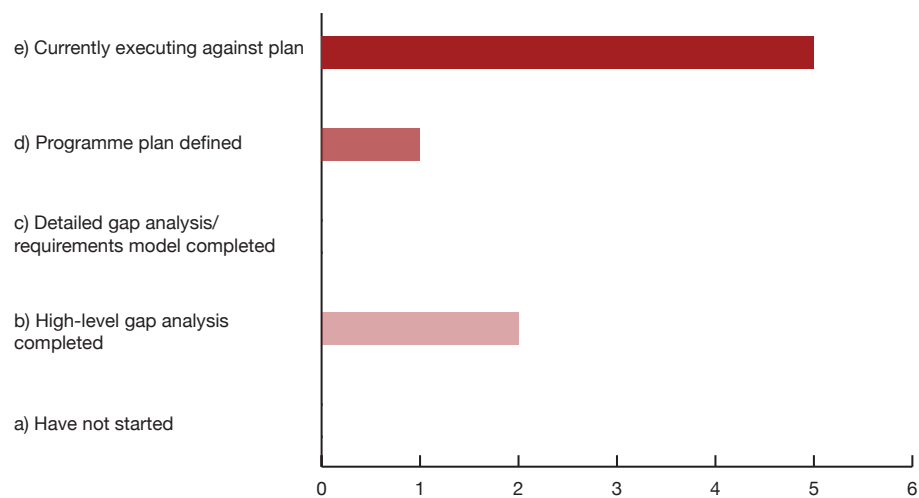


## Detailed survey questions and responses

### Question 1: What is your level of assessment and planning against the principles?

As can be seen below, of the eight respondents, five are currently executing against plan which includes addressing identified gaps or limitations (such as fixing data quality) and making data and systems architecture changes.

#### Response to level of planning and assessment



Eighty-three per cent of those respondents who are currently executing against plan confirmed that their execution involved data and system architecture changes.

The two banks who reported that they had only performed a gap analysis at that stage confirmed that, based on this gap analysis, they would be using their existing infrastructure to address the RDARR requirements and therefore did not anticipate significant data or system architectural changes.

#### Our view

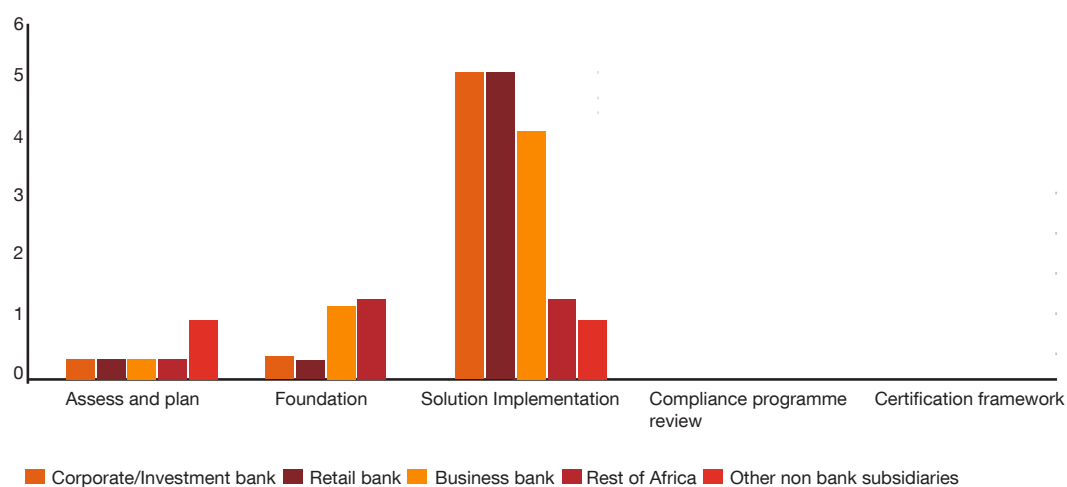
*Most of the banks have already designed plans and are executing against these plans. Project management and project assurance will be key in ensuring that these remain on course. Management need to guard against the programmes getting too complicated, too fast. Having a strong project assurance programme will ensure that the deliverables are prioritised and that interdependencies are adequately managed. Management need to be aware of scope creeps too. The changing needs of the business often outpace the agility of major programmes, causing frustration and delays. Changes to 'downstream' analytics requirements can have significant 'upstream' implications that need to be considered early, and thus firms need to consider new agile processes for solution delivery. Successful firms should embrace agile practices that allow end users of data to provide highly interactive inputs throughout the implementation process.*

**Question 2: At what stage of the implementation cycle would you say your organisation is currently for your various business units?**

The expectation by the SARB is that a bank should be able to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region and other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, risk concentrations and emerging risks.

In order to assess this, we asked the respondents at what stage of the implementation cycle they were at for each of their business units. Below is a summary of their responses:

**Stage of Implementation per business unit**



Most banks are currently at the solution implementation phase across most of their business lines. The focus at this stage is on the core business; as a result, work on the non-core businesses is either at a planning or foundation stage. The same holds true for most of the banks' Rest of Africa (RoA) subsidiaries. Work on these operations is expected to kick off in earnest only after 2017. For those banks who have considered some of their operations in the RoA as in scope for this initial phase of the project, this has mainly been driven by the significance of these entities to the group and by the need to achieve a certain level of coverage, e.g. risk-weighted assets (RWA).

None of the respondents selected had completed either a compliance programme review or a certification framework, as most of the respondents are currently busy with solution implementation and will only start focusing on these areas later in the year.

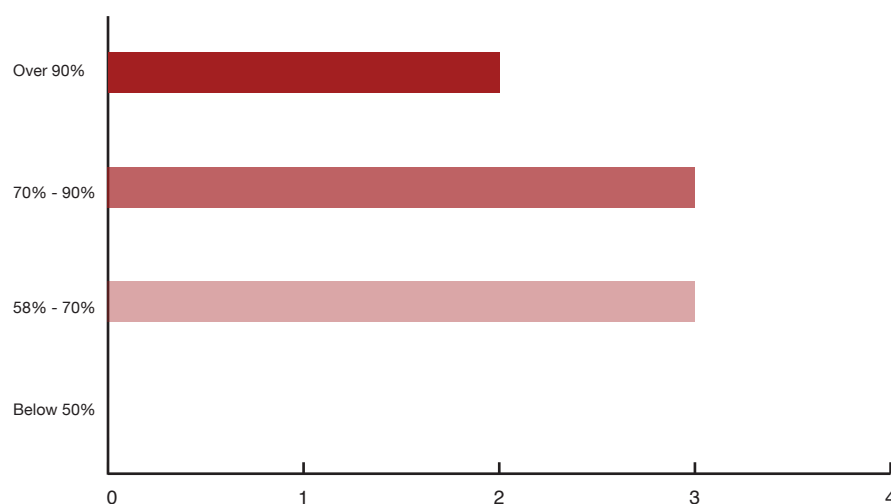
**Our view**

*The approach adopted by the SA banks is a pragmatic one and is in line with that adopted by many of the larger G-SIBs. It also allows for resources to be focused on areas that will yield the most benefit, and for banks to take lessons learned from this phase of the project to remaining operations once they get there. However, given their smaller size compared to their international counterparts, SA banks should be asking themselves whether there is scope or a supervisory expectation for them to be doing more.*

**Question 3: What is your assessment of your organisation's readiness to meet the 1 Jan 2017 deadline (if you have not answered (a) to question 1)?**

Considering the specific stage of implementation per business unit per bank, all banks indicated that as of March 2016, their overall readiness for the implementation date of 1 January 2017 was above 50%, as depicted below:

**Assessment of the banks' readiness to meet the 1 January 2017 deadline**



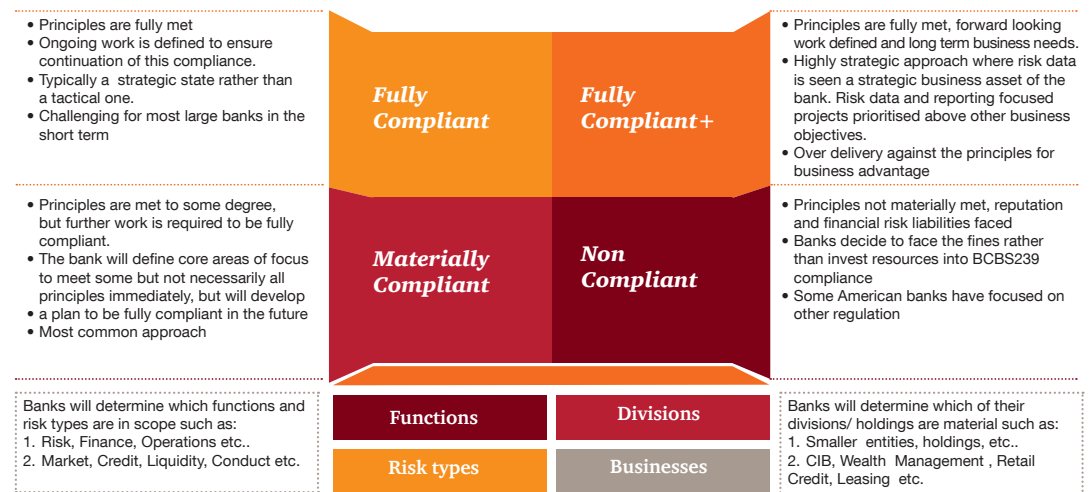
**Our view**

*It is important to note that the targeted state of compliance by the January 2017 deadline is dependent on what each bank has agreed with the regulator, which varies from bank to bank. The majority of the banks indicated that at this stage they have completed more than 70% of what they need to cover (according to their definition of compliance) in order to meet the 1 January 2017 deadline, and they were quite confident that they will meet their target state come January. However, most of the respondents noted that process automation will not have been achieved for all the areas currently in scope, and reliance will still be placed on manual controls and reconciliation in certain areas. Some of the key areas identified that will not have achieved the desired levels of compliance included remediation of data quality at source and independent validation. Fixing data quality at source is very challenging, due to legacy systems and also due to the difficulty in identifying the true source of data as this is reliant on data lineage which is complex and time consuming.*

**Question 4: What is your expectation of your level of compliance come 1 January 2017?**

It is important for banks to independently define their own compliant target state and their material entities considered in scope, and agree this with their regulator. In defining scope and compliance, we believe the terminology and definitions set out below would be useful in gaining a common understanding across the industry.

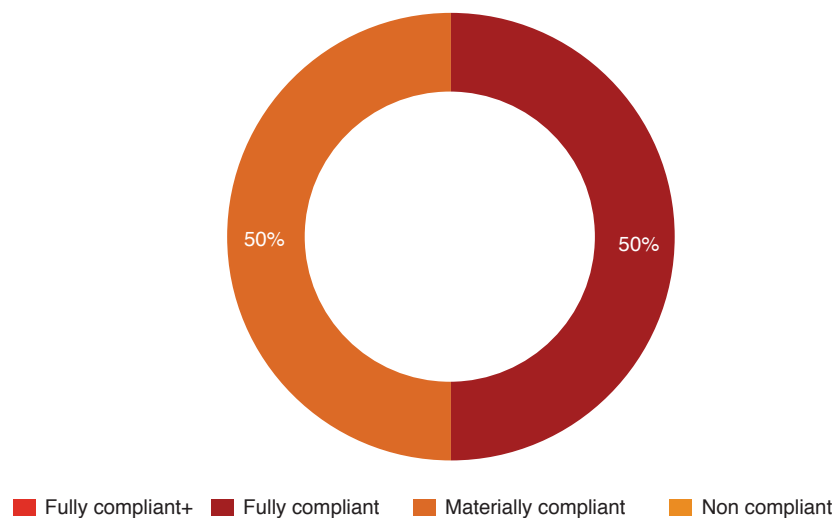
**Banks must define for themselves their compliant target state and the material entities in scope**



Source: Talking about BCBS 239 – Principles for effective risk data aggregation and risk reporting (PwC)

Based on the above definitions for the compliant target state, we asked the banks what their target state for 1 January 2017 was. As can be seen below, most banks selected either ‘materially compliant’ or ‘fully compliant’ as their target state.

**Target level of compliance**



The main reasons given for banks not being fully compliant + was that banks are initially looking to embed policies and processes, and aim to first achieve full compliance in this regard before pursuing longer-term plans. They will then follow this up with a full embedding process after the deadline of 1 January 2017.

The respondents believe that they will be compliant to the extent that some processes will not yet be fully automated by the due date; the alignment of documented policies and procedures is expected to still take place beyond 2017.

**Our view**

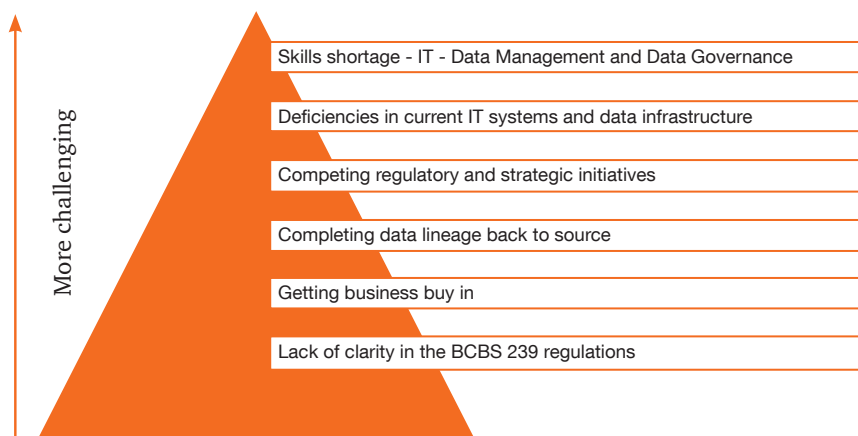
*The challenge to SA banks is whether they are thinking strategically enough about how to leverage the capabilities that full compliance will deliver. RDARR represents an opportunity to ‘dig up the road once’, and banks should be considering how RDARR can help them to mitigate the costs (and risks) of meeting future regulatory changes.*

*A second challenge that some UK banks have faced (and that SA bank should consider) is determining material compliance in the context of full compliance (that you can only get certainty that you’ve achieved material compliance – with limited work remaining – once you have clarity on what full compliance looks like for your organisation). It is not clear whether SA banks have considered this challenge when planning their own approaches.*

**Question 5: What is the biggest challenge you are experiencing now with regard to your implementation of BCBS 239?**

Based on the survey performed, the following key challenges have been ranked from most challenging to least challenging:

**BCBS 239 Challenges**



Skills shortage emerged as the major challenge faced by SA banks. Banks noted that technical skills around data governance, management and architecture were limited in the SA market. Another notable skill set in high demand was project management skills. Due to the limited supply of these skills, respondents noted that there was a high turnover of staff, which was slowing down the progress being made.



Legacy systems also remain a challenge that all the banks are grappling with as they seek to implement RDARR. As banks try to implement new solutions to comply with the BCBS 239 Principles, they are finding it difficult to extract the required information and automate the interfaces between the old systems and the new solutions. In the short term, most banks are targeting manual workarounds and reconciliations to solve this problem, with the intention being to replace these systems with automated solutions after the January 2017 deadline.

Respondents also noted that there are significant increases in the regulatory changes which they are also having to deal with, affecting areas such as IFRS 9, operational risk, stress testing and AML. For banks with limited risk teams this is proving to be a challenge as they strive to allocate these limited resources to various and competing needs. As a result, some banks have broken down the silos within their risk teams and are equipping them with skills to enable them to function in more than one risk type across the organisation. This allows for resources to be deployed and focused in the most pressing area at any given time.

#### **Our view**

*Skills shortages are probably lower down the priority list for the larger international banks, who have access to larger resource pools. However, access to subject matter experts within the organisation is still an acute challenge, particularly when tied to the demands of other competing regulatory change programmes for which the same individuals are relied upon. There is a lack of resources with specific data management experience, as typically this was the IT function's area of responsibility. The need for banks to establish formal data organisations with a dedicated CDO (Chief Data Officer) role has proven to be challenging.*

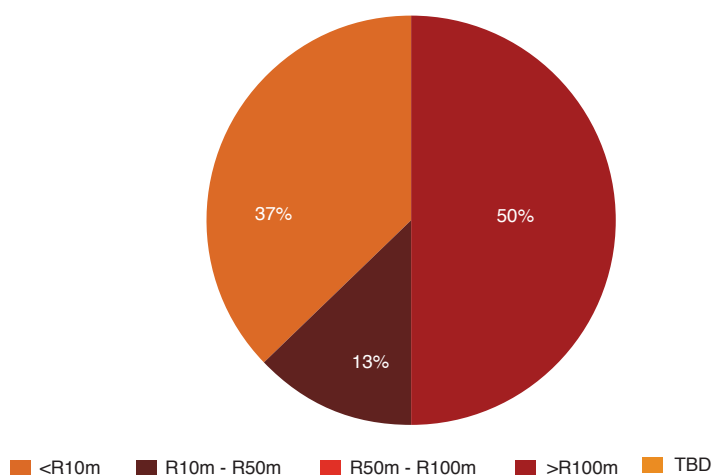
*A further challenge for global banks is how to continue making the business case for further investment in RDARR, given that there is a perception that it is yesterday's challenge and that the deadline has passed, with most banks claiming success. We predict SA banks will be faced with the same challenges in 2017, with supervisors keeping the spotlight on RDARR in the short term, but it remains to be seen how closely they will track compliance with the Principles alone, rather than considering them as a further requirement of other initiatives (e.g. this is the approach that the Federal Reserve has taken in the US, assessing BCBS 239 compliance through the annual Comprehensive Capital Analysis and Revenue (CCAR) stress tests.*



**Question 6: What is your estimated budget for the implementation of BCBS 239?**

In order to understand the cost implications of implementing BCBS 239, banks were asked what their estimated budget allocations were for the implementation of RDARR. 40% of the banks indicated that they could not split out the cost of BCBS 239, as this is not seen as a separate cost but rather as part of other initiatives that are currently being carried out. For example, one bank noted that it was upgrading its systems and IT environment, and was ensuring that the RDARR Principles were being taken into account in the process. RDARR costs were therefore absorbed as part of the overall costs in transforming the IT environment, and this bank indicated a total budget of less than R10 million for RDARR implementation. Most of the banks that were able to split this cost estimated that their spending would be in excess of R100m.

**Expected cost**



The banks estimating their implementation costs to be below R100 million indicated that they had systems in place that already aggregated risk data, and therefore no significant investments in this area were thought to be required. Furthermore, respondents noted that the amounts shown above was attributed solely to BCBS 239; however, all regulatory changes will result in overlaps, and the above excludes the view of what those potential overlaps may be.

**Our view**

*We would expect that the full cost associated with the implementation of BCBS 239 for the large SA banks to be well in excess of R100m. Similar to that for G-SIBs, this cost is expected to increase over the next three to five years as banks seek to remediate gaps identified and embed their strategic solutions across the whole entity. When estimating the investment that banks have made in achieving compliance with the Principles, it can be misleading, in our view, to only include specific programme costs, as investments are often already being made in a number of other areas. When communicating the level of investment to supervisors, banks should consider pulling together a more accurate representation of their total spend, including related initiatives, to demonstrate that they are not underspending relative to their peers. Furthermore, banks should be able to articulate to supervisors what they expect to spend in future on BCBS 239 as part of achieving full compliance.*



**Questions 7 & 8: Describe the key scope dimensions for your BCBS 239 programme, and have you excluded any areas from your scope?**

The main considerations by most respondents in determining their scope were:



Reports to board and executive management



Risk universe



Majority of African subsidiaries determined to be out of scope

Banks that had already decided on their risk metrics reported that as part of selecting these metrics they had considered all the significant risk types facing their business, including credit risk, liquidity risk, market risk, interest rate risk, operational risk etc. They had also considered all the reports submitted to their boards, executive management and the regulators, and the metrics included therein. Risks excluded from the project scope by all banks included conduct risk, reputational risk and strategic risk.

In terms of the legal entity coverage/geographic coverage, as highlighted in question 2 above, all the respondents are focusing on the operations that are expected to provide them with the highest level of coverage (most commonly this is defined as the proportion of total group RWA accounted for by the in-scope businesses). As a result, non-bank operations and non-material RoA subsidiaries, where applicable, have been excluded from the initial phase of the programme. The expectation is that these will be brought into scope after January 2017.

**Our view**

*The majority of G-SIBS took the decision to prioritise the scope of their BCBS 239 programmes to the most significant areas of their business due to the size, complexity and global footprint of their businesses. G-SIBS defined scope across a number of dimensions, including risk types, reports, metrics, businesses, geographies, products and customer segments. SA banks have included a larger proportion of their businesses within the scope of their RDARR programmes (commensurate with the scale of their operations), and are broadly in line with the global banks. However, two interesting areas have come into focus over the past one to two years for international banks: conduct risk and external reporting.*

*Conduct risk has become increasingly important in the wake of numerous mis-selling and rate-rigging scandals that have dominated headlines and that have led to sizeable regulatory fines. In this context, a number of banks have considered it as a new material risk type that should be subject to BCBS 239 requirements, and have added it into the scope of their compliance programmes (in some cases formally, in others informally via operational risk). Conduct is particularly challenging from an RDARR perspective due to the breadth of data required and the typically qualitative and non-aggregable nature of information. Given the increased focus that we expect will be placed on conduct once the FSB takes up its new role under the Twin Peaks model, SA banks need to already be thinking of how this will affect their programmes.*

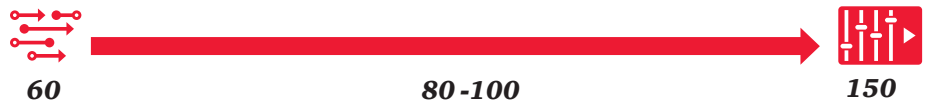
*Whilst the focus of BCBS 239 is clearly on internal management risk reporting, over the past two years supervisors have advised that they would also be looking at banks' regulatory returns (including stress testing) and disclosures as evidence of compliance. It was stated that if a bank's returns were either inaccurate or late, that would be considered non-compliance with the Principles. This has challenged banks significantly to widen the scope of the processes and controls to which RDARR standards need to apply. More fundamentally, it adds to the criticality of the requirement for risk and finance data to be reconciled and aligned, as the majority of regulatory reporting still remains the responsibility of the Finance function.*

**Questions 9 and 10: What is your expected scope in terms of number of metrics and underlying data elements, and is your priority breadth of metric coverage or depth of metric coverage?**

---

**Significant divergence in the number of metrics chosen**

---



As stated in BCBS 239, 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.

We asked the participating banks what their expected scope was in terms of the number of metrics and underlying data elements. We then asked whether, in defining this scope, priority was given to breadth of metric coverage (more metrics, less underlying data, and limited data lineage) or depth of metric coverage (less metrics but greater coverage of underlying data and lineage back to ultimate source), or both.

Despite the banks applying the same considerations in arriving at their metrics, as noted in question 7 above, there was a large variance in the number of metrics finally chosen by each bank, ranging from 16 metrics at one end of the spectrum to 150 metrics at the other. Even though the smaller banks tended to have fewer metrics when compared to their larger counterparts, the size of the bank was not necessarily a clear driver for this disparity. We noted disparity in the number of metrics chosen even amongst the larger banks. It's likely that these differences are down to the terminology and definitions being used (the same has been noted with international banks, and this is one of the reasons why it has been difficult to benchmark between banks).

The terminology and definitions employed are dependent on the needs of each specific bank and what has historically been reported to the executive management committee and board. While some organisations limited their metrics to those which were considered absolutely critical, others went into a bit more detail, therefore resulting in a higher number of metrics. Other potential drivers for the metrics chosen could be the structure of the bank's business (i.e. the level of autonomy with which the business units operate and the bank's geographical presence) and the nature of its operations.

On the question of depth or breadth, it was no surprise that the majority of the banks indicated that they paid equal attention to both depth and breadth. However, those banks that only indicated one factor as being important will need to consider whether the SARB will see them as outliers and as not having done enough in comparison to their peers.



### Our view

*Inconsistent terminology across the industry has been one of the bigger challenges for banks in sharing information and learning from the practices of peers (as is recommended in the December BCBS 239 progress update). Global banks have commissioned PwC to conduct a more detailed benchmarking of data scope for BCBS 239. SA banks should also consider whether a similar exercise would be of value to them.*

*Regarding the depth of data lineage, most global banks have elected to focus on breadth first rather than depth due to the volume of data they hold. Typically, this has meant only conducting data lineage back to the point of entry into risk and finance, or back to the source system for a metric, rather than continuing to trace back the underlying data elements that are used to calculate it to the true source. The G-SIBs that have conducted full end-to-end lineage have only done so for a small number of metrics. Full data lineage is time consuming and resource intensive. However, it is essential if banks are to fully identify and remediate the root causes of underlying data quality issues.*

### Question 11: How do you define success for BCBS 239 compliance?

We believe that there are aspects of BCBS 239 for which banks must be in a position to demonstrate that they are unambiguously compliant (the ‘non-negotiables’) come January 2017. These are summarised below:

Aspect	Key consideration
	<b>A. Governance</b> <ul style="list-style-type: none"><li>• Board-level sign-off of material compliance and full compliance scope</li><li>• Fully engaged board in defining risk reporting requirements</li><li>• Risk data governance, policies and operating model fully operational</li><li>• Certification / attestation of existing and future capabilities</li></ul>
	<b>B. Architecture and Infrastructure</b> <ul style="list-style-type: none"><li>• Established strategic sourcing strategy and roadmap to achieve</li><li>• Complete risk data taxonomy, dictionary – aligned with enterprise data model, data management framework/policy and operating model</li><li>• Roadmap and plan established for strategic risk architecture; making progress</li><li>• Data quality baseline established, monitoring in place</li></ul>



### C. Data Aggregations

- Risk data (key risk data elements) definition, standards and quality measures established
- End-to-end data lineage completed – tactical remediation complete; strategic solution roadmap defined and making progress
- Reconciliation controls established, reviewed and attested to

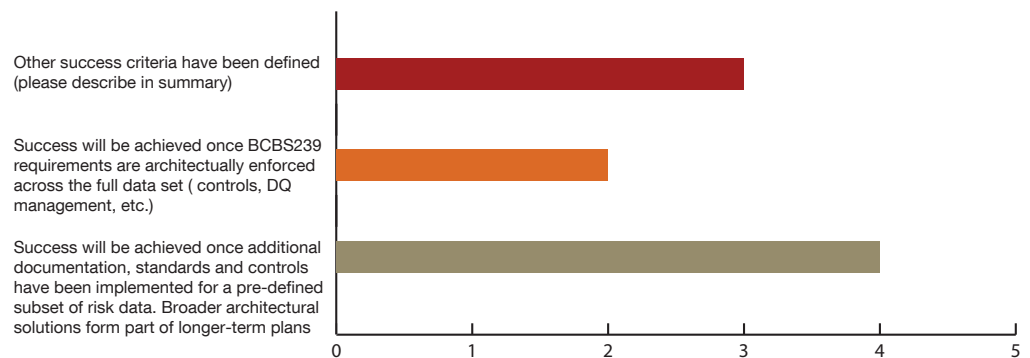


### D. Reporting

- Board-level and other senior risk management fora reports catalogued, documented, assessed and improved where required
- Reporting metrics agreed and standards defined. All reporting processes reviewed, documented and control evidenced across normal-basis risk reporting, stress-basis reporting and regulatory reporting
- Stress and crisis reporting procedures established and tested

Based on the above table, banks were then asked what they would define as success for their specific BCBS 239 implementation. Almost all the banks were in agreement that success would have been achieved once additional documentation, standards and controls have been implemented for a pre-defined subset of risk data. Broader architectural solutions form part of longer-term plans for most banks. Only two banks indicated that success would be achieved once the BCBS 239 requirements are architecturally enforced across the full data set (controls, DQ management, etc.).

#### Success as defined by banks



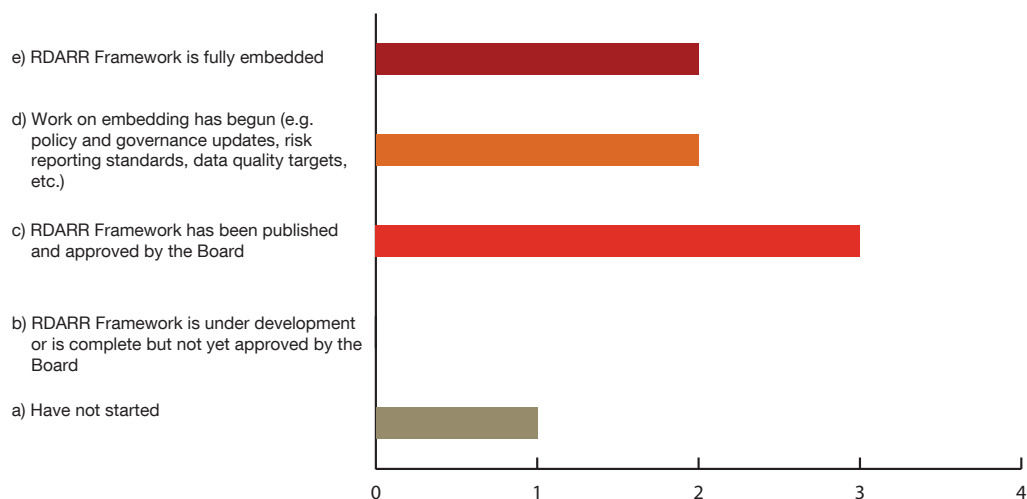
\* One of the respondents provided two answers

Other success criteria determined by banks include meeting the SARB deadline and being materially compliant.

**Question 12 and 13: To what extent have you defined and embedded your RDARR framework, and to what extent do you need to improve your current-state documentation?**

All the banks except for one confirmed that they had an RDARR framework in place that had already been approved by their boards. Fifty per cent of the banks indicated that work on embedding this framework was underway or was already complete. There are several challenges that are being experienced as banks undertake their embedment process. The levels of embedment have been found to be different within different businesses within the same organisation. Organisations are also yet to decide on what is the best way to demonstrate compliance with BCBS 239 and a successful embedding of their RDARR framework.

**Definition & Embedding of RDARR framework**

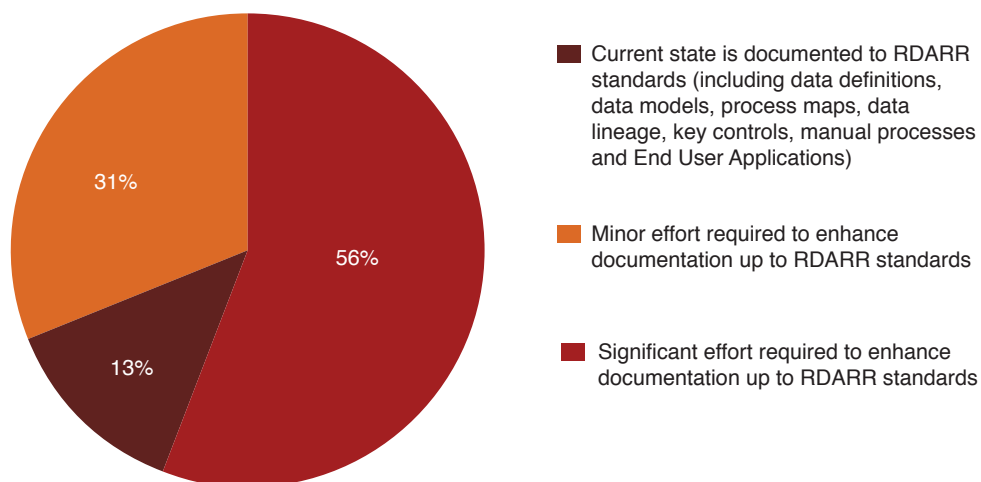


The banks were asked to comment on the state of their existing documentation across their organisation. The majority of banks believe that significant effort is required to enhance documentation to meet RDARR standards. Certain banks noted that even though some BCBS 239 Principles were already in existence, these were not adequately documented or not documented at all. Two of the banks interviewed were comfortable with their current documentation and indicated that only minor effort is required to bring it in line with the Principles set out by the Basel Committee.

---

## Current documentation status

---



### **Our view**

*Documentation is key in evidencing compliance, both internally and externally, and there has been an increased focus from banks in this area. Specific attention is being paid to enhancing documentation around data definitions, data mapping and data lineage controls.*

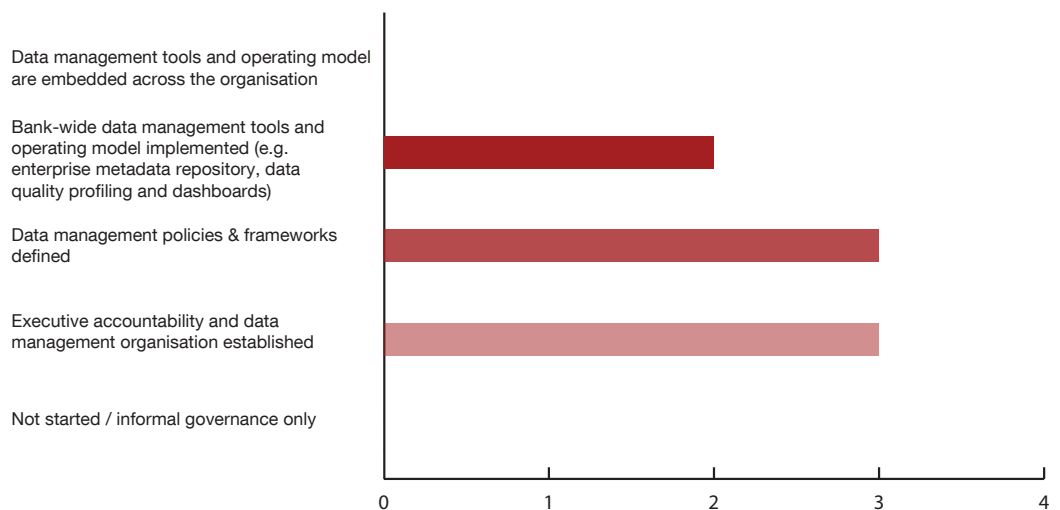
*The BCBS 239 Principles are clear on the enhancements that banks are required to make to the governance and control environments that support their risk data aggregation and reporting. In many cases international banks have underestimated the level of effort required to develop a standardised set of documentation, aligned to a new RDARR framework document. In order to support and enable ongoing compliance, new standards need to replace old ones, often necessitating changes to procedures and ways of working. New documentation also needs to satisfy independent validation and compliance assessments by second and third-line-of-defence teams. Process maps, data lineage diagrams and control inventories also need to be stored in new repositories with appropriate access controls and kept up to date. Global banks are only now considering how best to meet these challenges, and SA banks should not underestimate this key requirement.*

**Question 14: To what extent have you established bank-wide data governance?**

As per the BCBS 239 Principles a bank’s board and senior management should promote the identification, assessment and management of risks relating to data quality inaccuracies as part of their overall risk management framework. The framework should include agreed service level standards, for both outsourced and in-house risk data related processes, policies on data confidentiality, integrity and availability, as well as its risk management policies.

All the banks interviewed have a data governance process in place, however, the banks were at various stages of maturity. This is expected to align over time as their implementation matures. Banks are working towards achieving consistency in the quality of documentation and data governance across the business lines. This means challenging the autonomy with which some of the businesses (e.g. retail vs corporate) have been operating.

**Established data governance**



Though the majority of the banks who participated in this survey do not have an active CDO, the lack of such experience in the South African market does not deter these banks from ensuring that the requirements of the role are fulfilled elsewhere.



### Our view

The importance of data is now being recognised by members of the board and senior management across the banks; and due to regulations such as BCBS 239, there is an increasing need for banks to establish formal data organisations. In early 2013, the majority of G-SIBs were either in the process of setting up a data management organisation or had explicitly established one as a result of the BCBS 239 Principles. At the time there was growing recognition of the importance of data within the organisation and the need to fix the endemic problem of poor data quality.

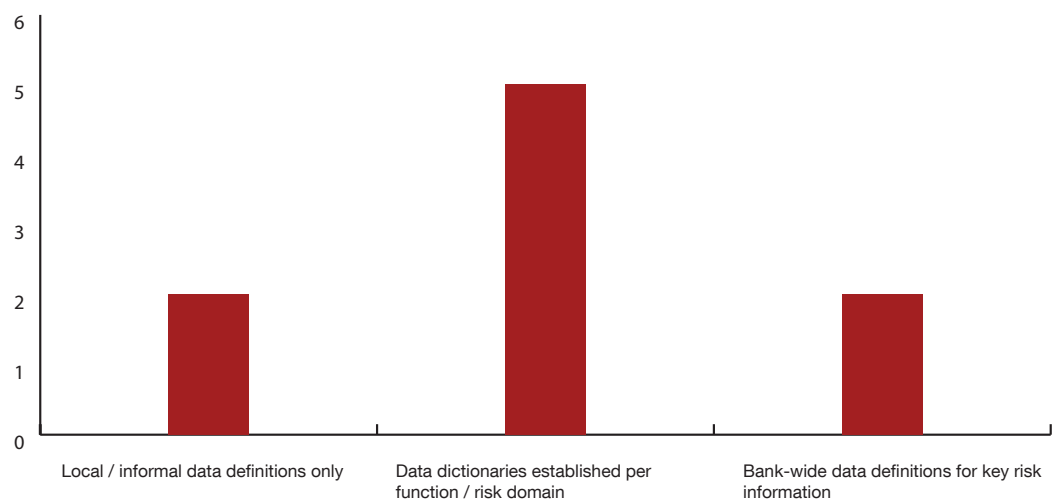
The CDO role is evolving from a reporting line, scope and responsibility perspective as regulatory requirements (e.g. BCBS 239, data-linked add-ons to capital and liquidity charges, increased focus on transaction reporting and the advent of legal entity identifiers) are driving the need for clear ownership of and accountability for data across the enterprise. CDO responsibilities vary by organisation, but will typically cover governance (data owners, stewards, process, operating model) and, in some cases, both architecture (data integration, data warehousing, reporting, reference data) and shared solutions BI COE (Business intelligence centre of excellence), common platform, standards tools). The majority of firms choose governance as the core responsibility of a CDO, and the first step is to establish an effective governance framework. The transition to an enterprise-wide scope increases the complexity and cost of coordinating governance and architecture across business units and corporate functions. An initial investment is required, however, many organisations believe a positive ROI will be realised in the long run.

### Question 15: To what extent have you established bank-wide data definitions?

According to the RDARR Principles, banks should be able to generate accurate and reliable risk data to meet business as usual, stress or crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors. As a precondition, a bank should have a 'dictionary' for the concepts used, such that data is defined consistently across the organisation.

When we asked the banks whether they had established bank-wide data definitions, we received mixed responses, with the majority of respondents indicating that they had established data dictionaries per function and some banks having created bank-wide and local definitions.

#### Level of established bank-wide data definitions



\* For the above question, one of the respondents selected two options

We noted that the majority of banks have data dictionaries per function. However, more work needs to be done to ensure bank-wide data definitions for risk information are established and embedded across the organisation.

**Our view**

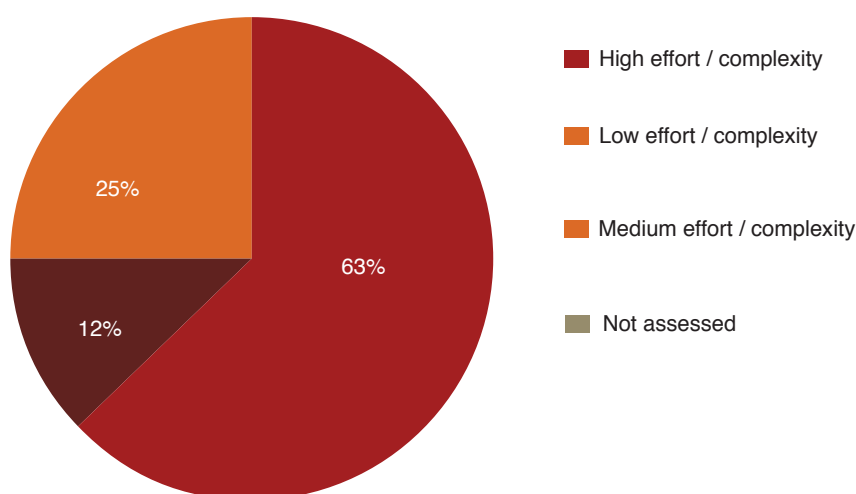
*The lack of a single source of bank-wide and common data definitions is a significant restriction in the aggregation of risk data across the bank. RDARR promotes the need for senior management and boards (at group level) to see a single aggregated view of their risk profile – such as a single customer view. We believe that South African banks need to do a lot more work in this area to ensure that group-wide definitions are achieved.*

**Question 16:  
How much effort / complexity is required to adopt single identifiers / common reference data?**

BCBS 239 requires banks to establish integrated data taxonomies and architectures across the banking group which include information on the characteristics of the data (metadata), and use single identifiers and/or unified naming conventions for data, including legal entities, counterparties, customers and accounts.

Based on the responses received from banks, we noted that a high level of effort would be required by the majority of the banks to adopt single identifiers or common reference data.

**Effort/Complexity required to adopt single identifiers/common reference data**



**Our view**

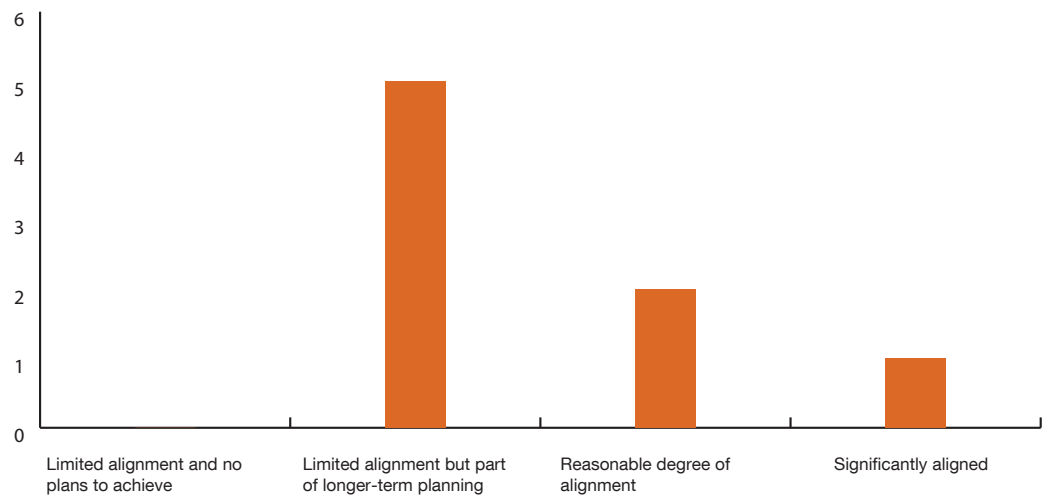
*This is undoubtedly the most challenging requirement in BCBS 239, and the majority of G-SIBs have longer-term initiatives in place to achieve compliance. A further challenge of this requirement is that although it's part of Principle 2 (Data Architecture and Infrastructure), it's also a more fundamental enabler of many of the other BCBS 239 requirements (such as enhancing adaptability, enabling cleaner reconciliations, and proving the basis for greater automation of processes end-to-end). As such, it could be considered as a prerequisite to compliance with a much broader range of Principles; however, the majority of banks have de-coupled fully meeting this requirement from meeting other Principles.*

*Global banks have selected priority reference data items (such as customer/counterparty and product) and have developed target data architectures and roadmaps to enable enterprise data distribution and the adoption of reference data. Many banks are also keeping a close eye on emerging service offerings in the managed service/utility provider space to significantly reduce the expense of maintaining reference data.*

**Question 17: To what extent have you achieved or are you planning to achieve risk and finance alignment?**

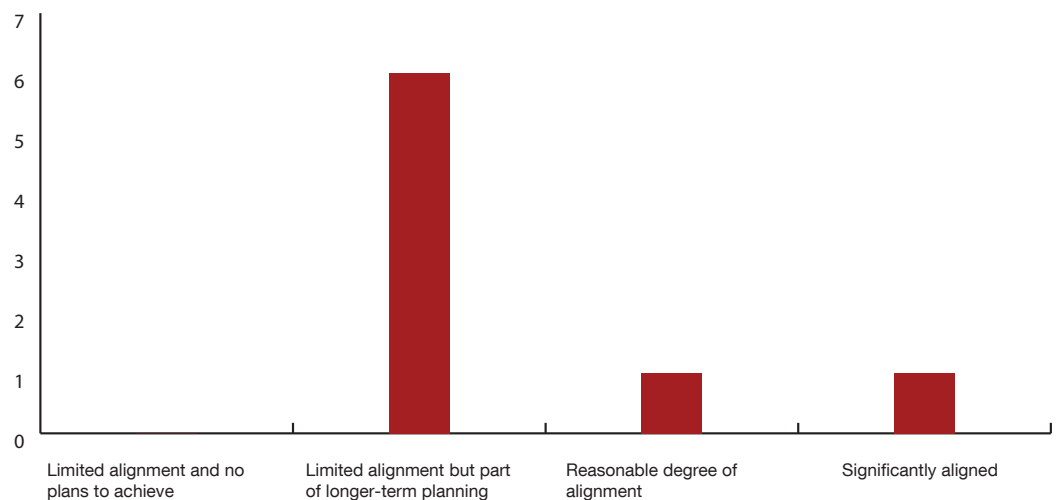
A key BCBS 239 requirement is the alignment of risk and finance data, which is at the core of the RDARR Principles. The survey revealed that this is an area of significant challenge for most banks as they recognise the importance of achieving alignment, not only to be compliant, but as a step towards improved risk management. Banks also noted the efficiency to be gained by ensuring alignment between risk and finance, as this ensures that some of the key metrics need only be calculated once and can then be relied on by both teams.

**Risk and Finance alignment - Integrated data models**



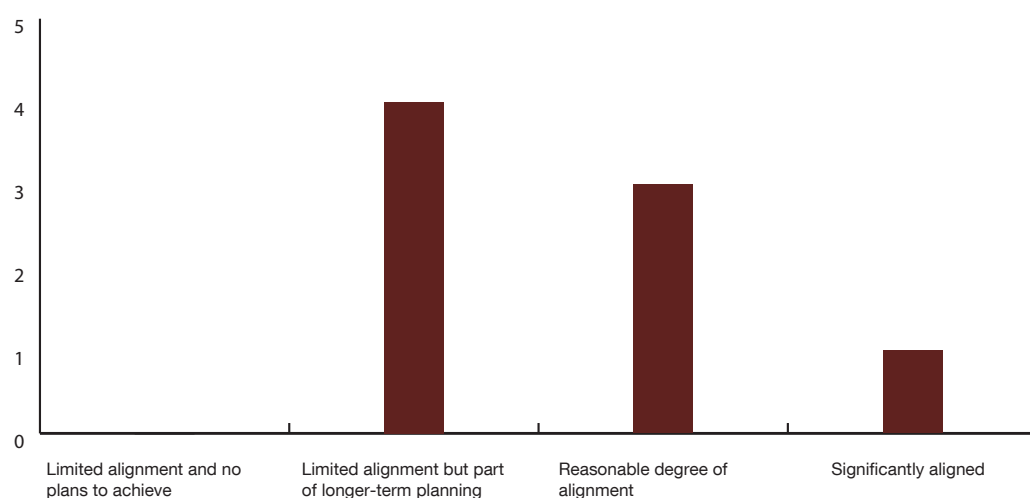
From all the banks interviewed, only one indicated that they had achieved significant integration between the risk and finance data models. The majority of respondents, although reporting limited alignment at this stage, are expected to achieve full alignment as part of their long-term goals. This is mainly the case for banks that are making significant system enhancements (including the implementation of new systems).

**Risk and Finance alignment - Architectural governance and roadmap**



The challenges banks are facing with respect to their architectural governance and data lineage, as well as, IT skills shortage are having a knock on effect in terms of their ability to achieve significant alignment. Interesting to note, the banks that have not made any major system changes, still managed to achieve significant alignment in their architectural governance and roadmap to align risk and finance. Most of the banks are not expected to achieve alignment (or will just achieve limited alignment) of risk and finance by the deadline date. However, these banks believe that this will be achieved in the long run.

### Risk and Finance alignment - Externally reported risk information



When it came to externally reported risk information, only three banks reported that they had achieved reasonable to significant alignment. The majority of the banks expect this alignment to be achieved in the long term.

Major challenges cited by the respondents included multiple sources of both risk and finance data, independence and a silo approach stemming from the fact that most risk and finance functions have evolved separate, legacy systems (both in risk and finance, both of which have historically operated independently of one another) and data reconciliation difficulties. In response to these challenges, most of the respondents are making significant investments in new systems that are integrated and that address both the adoption of bank-wide data definitions (for use across both risk and finance) and the creation of single data identifiers across the whole organisation.

#### Our view

*The financial crisis has changed the way that banks look at risk and finance integration, and there has been increased support for closer alignment of these two functions. Financial institutions are under pressure to deliver improved and more transparent management information reporting whilst at the same time reducing costs within the constraints of internal factors such as liquidity and capital capacity, and external factors such as regulatory requirements. Meeting these demands requires close coordination between risk and finance functions. This is discussed in greater detail in PwC's risk/finance convergence whitepaper, "Blurring the lines between risk and finance", published in December 2014.*

*Bringing finance and risk together has always been easier said than done, but as the case for greater alignment becomes more compelling and the momentum for change increases, banks locally and internationally are beginning to see real progress. Rather than building alignment around systems or attempting to bolt disparate functions together, a fresh approach is emerging. The starting point is a top-down vision for the functions based on what capabilities are required now and in the future, what outcomes they should achieve, and what process and organisational steps would enable them to get there.*

*Clearly, alignment presents challenges stemming from different mandates, backgrounds, skills, processes and underlying technology. But looking at where you want to be rather than where you've come from allows teams to put these differences aside and mobilise around a common goal. Any firm that aims to comply with the letter and the spirit of BCBS 239 will need to consider how to fully implement straight-through processing with minimal touch points, the removal of reconciliations and reporting errors, and a risk and finance group using the same data and controls under a revised operating model.*

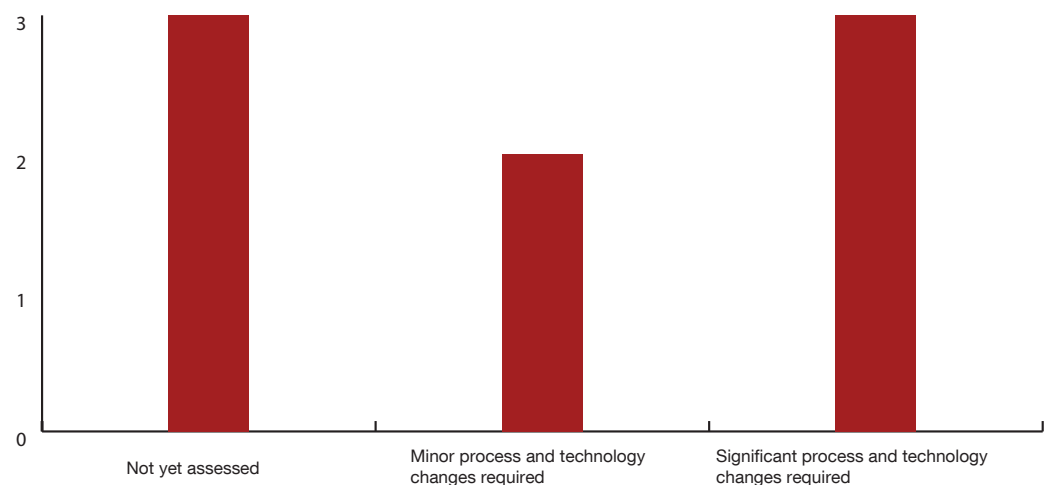
*The majority of international banks have not tackled full risk and finance integration or alignment as part of their BCBS 239 programmes, due to the scale of change required. However, there are a variety of approaches to this problem. Most banks have taken the opportunity to put greater controls around the handshake between risk and finance, where data is passed between the functions. In some cases, service level agreements (SLAs) have been established for each data flow between data producers and consumers in the risk, finance and treasury functions. A smaller number of banks took the initiative to establish combined risk and finance data aggregation or reporting teams, in most cases with little or no system changes. In most cases this has led to reductions in the time taken to produce risk data and reports.*

**Question 18: What is the level of impact to meet stress/crisis period reporting requirements?**

The banks' ability to report and assess the impact of stress scenarios has received some focus recently. When the respondents were requested to assess their readiness to respond and report in periods of stress, a third of the banks indicated that they had not assessed that at this stage. Banks also indicated that they were waiting for guidance from the SARB on what their expectation was of the work to be performed in this area.

Based on preliminary assessments done by banks, most believe that some process and technology changes will be required to enable them to meet these reporting requirements.

**Stress/Crisis period reporting requirements**



### Our view

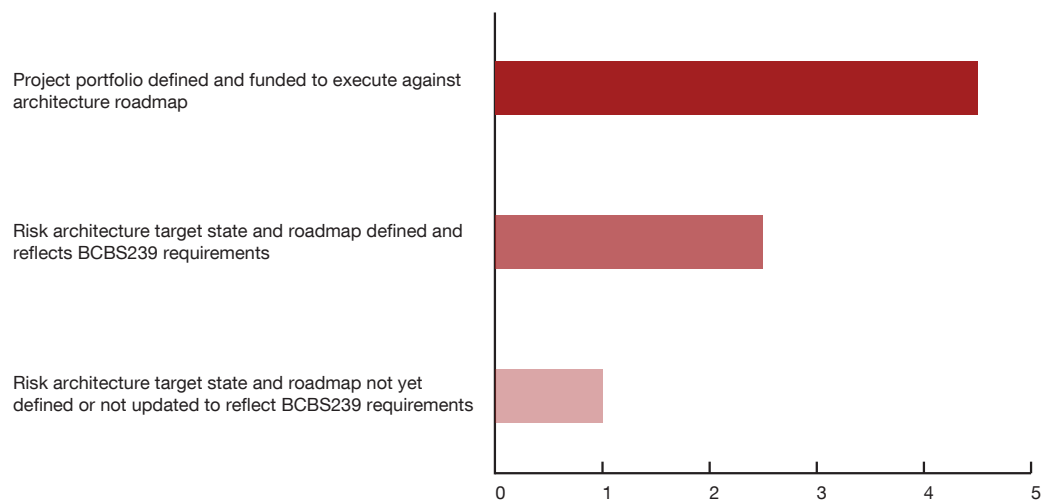
Whilst most banks have achieved efficiency and timeliness improvements through greater controls and the formalisation of processes, roles and responsibilities, step changes in stress/crisis or ad hoc reporting capabilities are only fully enabled by significant data and architectural changes. Report production timelines are typically constrained by a combination of technology barriers (e.g. multiple batch-load processes and reliance on end-user-developed applications) and manual processes (e.g. data cleansing, top-level adjustments, extensive approval and sign-off chains). Most G-SIBs expect to realise these benefits as part of continual improvement through the ongoing delivery of their architecture roadmap.

To achieve BCBS 239 compliance, many international banks have focused on the development of stress/crisis 'playbooks', comprising standards for data aggregation and reporting under stress/crisis situations or for ad-hoc requests, and procedures to be followed. Standards typically include the acceptable trade-offs between accuracy, completeness and timeliness, and specific data quality thresholds for key metrics required. Procedures would include required roles and responsibilities, action groups, and data elements that would be needed under a range of potential events – typically assessed by risk type. Compliance was evidenced through the testing of playbooks to determine that procedures could be followed and required data standards could be achieved.

### Question 19: To what extent have you established an architecture roadmap to meet BCBS 239 requirements?

In accordance with the requirements of BCBS 239, 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.

#### Architecture roadmap



Most of the banks indicated that a project portfolio has been defined and funded to execute against an architecture roadmap. Roles and responsibilities should be established as they relate to the ownership and quality of risk data and information for both the business and IT functions. The owners (business and IT functions), in partnership with risk managers, should ensure there are adequate controls throughout the lifecycle of the data and for all aspects of the technology infrastructure.

### **Our view**

*Prior to 2013, most international banks were already thinking about or developing their long-term IT strategies; however, the level of commitment to technology spend at board level varied significantly. Some banks had already invested large sums in technology programmes that had not delivered, but most were still focused on front-office and business systems rather than their more sizeable and problematic back-office architectures. For many banks BCBS 239 was the catalyst for launching planned technology initiatives, as it provided a mandatory and regulatory imperative that had not previously existed.*

*Many G-SIBs have communicated to their supervisors that full implementation of an architecture roadmap that meets the Principle 2 requirements will be a multi-year journey that extends beyond the original compliance deadline. This message is acknowledged in the Basel Committee progress paper published in December 2015. However, it is also clear that banks must be able to demonstrate clear progress in upgrading their IT infrastructures, and they must be able to articulate when they expect to have fully met the standard. To achieve this, G-SIBs have added RDARR into their IT strategy and roadmaps, but they have also executed incremental improvements to their existing systems. These have included consolidating and rationalising data feeds into risk systems; addressing siloed data stores and defining golden sources of data; upgrading reporting platforms to deliver more timely information; and implementing vendor business intelligence solutions for rapid reporting.*

*Many banks were already considering or had embarked upon the creation of a common data repository for key areas of data (such as a credit risk data warehouse or trade data repository). However, few banks had successfully made the case for more fundamental architecture changes such as integrated risk and finance repositories, common reference data stores or bank-wide unified data models. Since then, continued regulatory scrutiny around BCBS 239 and the need for banks to reduce data management costs and adapt to a leaner operating environment have strengthened the argument for long-term strategic investment. Recognising the central importance of an enterprise data model and supporting data architecture, most banks have established plans to develop an enterprise data layer, including enterprise data warehouses and data integration/distribution tools. Furthermore, banks are looking to use these technologies to enable wider benefits through the adoption of Big Data technologies. Terms such as ‘data lake’ and ‘data fabric’ are now commonly used to describe the ubiquitous access to data that should be enabled by target-state architectures.*



**Question 20: Who do you plan to rely on for quality control/to get bank boards and regulators over the line?**

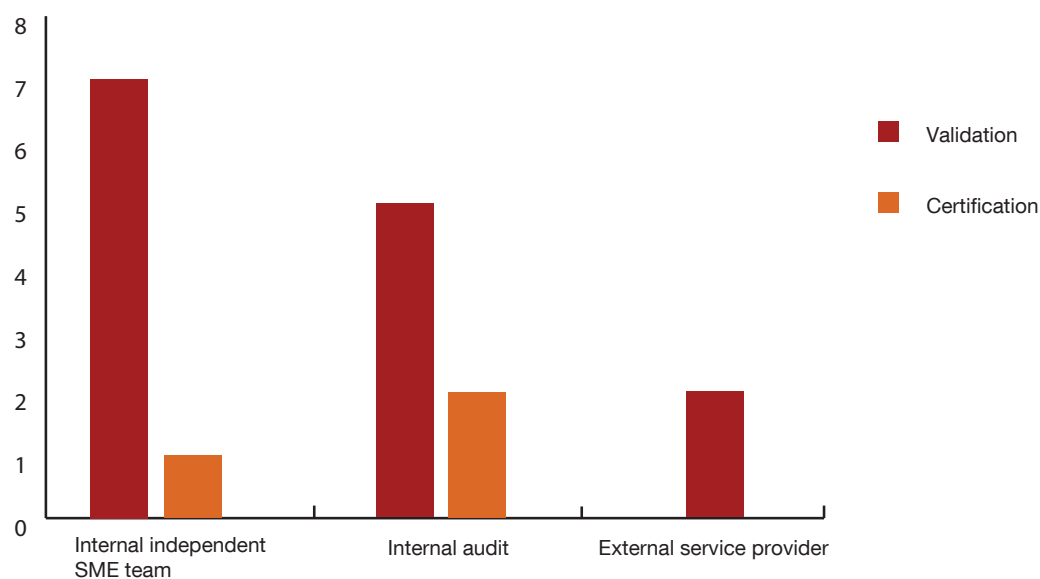
Principle 12 of BCBS 239 indicates that supervisors should periodically review and evaluate a bank's compliance with the eleven Principles of RDARR. Supervisors are required to draw on reviews conducted by the internal or external auditors to inform their assessment of compliance with the Principles. Supervisors may require work to be carried out by a bank's internal audit function or by experts independent from the bank. The Principle also requires that supervisors have access to all appropriate documents, such as internal validation and audit reports, and that they should be able to meet with the external auditors or independent experts from the bank to discuss risk data aggregation capabilities, when appropriate.

The majority of respondents to the survey indicated that internal auditors and independent internal SME teams would be leveraged to perform certification and validation of BCBS 239 compliance.

---

**Quality Control**

---



### **Our view**

*The majority of G-SIBs are currently preparing for either direct supervisory reviews or deep dives from their own internal audit functions at the request of national supervisors. A key challenge in this is determining how to gather appropriate evidence to demonstrate that compliance – as they have defined it – has been achieved for each of the Principles. Some banks are requiring senior business stakeholders to attest that compliance requirements have been achieved. Other approaches include the communication of improvements in capabilities, such as improved data quality or faster reporting. However, in order to demonstrate compliance across all Principles, we have assisted banks in developing a compliance certification framework. This comprises capability-based criteria, supported by a detailed rules set, mapped directly back to the Principles and underlying paragraphs. In some cases, this framework is also being adopted as part of the ongoing independent validation framework.*

*The establishment of an independent validation function in the second line of defence, to assess ongoing compliance status, is a specific requirement of the Principles. In most cases banks have sought to add this responsibility to existing assurance teams (e.g. as part of operational risk, risk operations, or where a separate risk assurance team is already in place) rather than creating a new dedicated function. New second-line validation responsibilities also have to be aligned to internal audit activities, with review schedules being aligned to ensure that compliance reviews are not conducted on the same business areas or processes concurrently.*

*In our view, once BCBS 239 programmes have transitioned into business-as-usual, there will need to be an ongoing RDARR oversight office (similar to SOx teams). This office will provide ongoing BCBS 239 expertise, advise on new regulatory developments, provide guidance on future change programmes, and facilitate the annual communication of compliance status to national supervisors.*

## **Appendix 1: Survey questionnaire**

### **Question**

---

**1. What is your level of assessment and planning against the Principles?**

- a.** Have not started
- b.** High-level gap analysis completed
- c.** Detailed gap analysis / requirements model completed
- d.** Programme plan defined
- e.** Currently executing against plan (if selected refer to 'Question 1e' tab)

---

**2. At what stage of the implementation cycle would you say your organisation is currently for the respective business units?**

- a.** Have not started
- b.** High-level gap analysis completed
- c.** Detailed gap analysis / requirements model completed
- d.** Programme plan defined
- e.** Currently executing against plan (if selected refer to 'Question 1e' tab)

---

**3. What is your assessment of your organisation's readiness to meet the 1 Jan 2017 deadline (if you have not answered (a) to question 1)?**

- a.** Below 50%
- b.** 50% - 70%
- c.** 70% - 90%
- d.** Over 90%

---

**4. What is your expectation of level of compliance come 1 January 2017 (refer to question 4 for definitions)?**

- a.** Fully compliant +
- b.** Fully compliant
- c.** Materially compliant
- d.** Non-compliant

---

**5. What is the biggest challenge you are experiencing now with regard to your implementation of BCBS 239 (feel free to select more than one selection and rank the ones selected with 1 being the most challenging)?**

- a. Skills shortage - specify skill type
- b. Getting business buy in
- c. Competing regulatory and strategic initiatives - specify key initiatives
- d. Deficiencies in current IT systems and data infrastructure - specify
- e. Completing data lineage back to source
- f. Lack of clarity in the BCBS 239 regulations - specify which areas

---

**6. What is your estimated budget for the implementation of BCBS 239?**

- a. <R10m
- b. R10m - R50m
- c. R50 - R100m
- d. >R100m

---

**7. Please describe the key scope dimensions for your BCBS239 programme, if known:**

- Material risks:
- Risk reports:
- Business:
- Geographic / Legal Entity coverage:

---

**8. Have you excluded any areas from your scope? If so please list and the reasons for exclusion**

---

**9. What is your expected scope in terms of number of metrics and underlying data elements?**

- Number of metrics:
- Number of underlying data elements

---

**10. Is your priority breadth of metric coverage (more metrics, less underlying data, limited data lineage) or depth of metric coverage (less metrics but greater coverage of underlying data and lineage back to ultimate source)**

- a. Greater breadth, less depth
- b. Greater depth, less breadth
- c. Both are equally important

---

**11. Broadly, how do you define success for BCBS 239 compliance?**

- a. Not yet agreed
- b. Success will be achieved once additional documentation, standards and controls have been implemented for a pre-defined subset of risk data. Broader architectural solutions form part of longer-term plans
- c. Success will be achieved once BCBS239 requirements are architecturally enforced across the full data set (controls, DQ management, etc.)

- d.** Other success criteria have been defined (please describe in summary)

---

**12. To what extent have you defined and embedded your Risk Data Aggregation and Risk Reporting (RDARR) Framework?**

- a.** Have not started
- b.** RDARR Framework is under development or is complete but not yet approved by the Board
- c.** RDARR Framework has been published and approved by the Board
- d.** Work on embedding has begun (e.g. policy and governance updates, risk reporting standards, data quality targets, etc.)
- e.** RDARR Framework is fully embedded

---

**13. To what extent do you need to improve your current state documentation?**

- a.** Current state is documented to RDARR standards (including data definitions, data models, process maps, data lineage, key controls, manual processes and End User Applications)
- b.** Minor effort required to enhance documentation up to RDARR standards
- c.** Significant effort required to enhance documentation up to RDARR standards

---

**14. To what extent have you established bank-wide Data Governance?**

- a.** Not started / informal governance only
- b.** Executive accountability and data management organisation established
- c.** Data management policies & frameworks defined
- d.** Bank-wide data management tools and operating model implemented (e.g. enterprise metadata repository, data quality profiling and dashboards)
- e.** Data management tools and operating model are embedded across the organisation

---

**15. To what extent have you established bank-wide data definitions?**

- a.** Local / informal data definitions only
- b.** Data dictionaries established per function / risk domain
- c.** Bank-wide data definitions for key risk information

---

**16. How much effort / complexity is required to adopt Single Identifiers / common reference data?**

- a.** Not assessed
- b.** Low effort / complexity
- c.** Medium effort / complexity
- d.** High effort / complexity

---

**17. To what extent have you achieved or are you planning to achieve Risk and Finance alignment across:**

17.1 Integrated data models

17.2 Architectural governance and roadmap

17.3 Externally reported risk information

- a.** Limited alignment and no plans to achieve
- b.** Limited alignment but part of longer-term planning
- c.** Reasonable degree of alignment
- d.** Significantly aligned

---

**18. What is the level of impact to meet Stress / crisis period reporting requirements?**

- a.** Not yet assessed
- b.** Minor process and technology changes required
- c.** Significant process and technology changes required

---

**19. To what extent have you established an architecture roadmap to meet BCBS239 requirements?**

- a.** Risk architecture target state and roadmap not yet defined or not updated to reflect BCBS239 requirements
- b.** Risk architecture target state and roadmap defined and reflects BCBS239 requirements
- c.** Project portfolio defined and funded to execute against architecture roadmap

---

**20. Who do you plan to rely on for quality control/to get bank boards and regulator over the line?**

- a.** Internal independent SME team
- b.** Internal audit
- c.** internal service provider

## Appendix 2: Summary of the BCBS 239 principles

<p><b>Impact assessment</b></p>  <p>High Medium Low</p>	<p>1. Governance</p> <ul style="list-style-type: none"> <li>• Board oversight</li> <li>• Awareness of limitations</li> <li>• Data governance</li> <li>• Documentation &amp; validation</li> <li>• Resilience</li> </ul>	<p>2. Data architecture &amp; IT infrastructure</p> <ul style="list-style-type: none"> <li>• IT Vision and roadmap</li> <li>• Data model</li> <li>• Data taxonomies</li> <li>• Meta data &amp; data lineage</li> <li>• Data ownership</li> </ul>	<p>3. Accuracy &amp; integrity</p> <ul style="list-style-type: none"> <li>• Golden data sources</li> <li>• Data dictionary</li> <li>• Aggregation methods</li> <li>• Control framework</li> <li>• Process automation</li> <li>• End user computing</li> </ul>
<p>4. Completeness</p> <ul style="list-style-type: none"> <li>• Self-assessment</li> <li>• Data monitoring</li> <li>• Implementation controls</li> </ul>	<p>5. Timeliness</p> <ul style="list-style-type: none"> <li>• Self-assessment</li> <li>• Critical risk data</li> <li>• Remediation activities</li> </ul>	<p>6. Adaptability</p> <ul style="list-style-type: none"> <li>• Flexible aggregation</li> <li>• Flexible reporting</li> <li>• Data availability</li> <li>• responsiveness</li> </ul>	<p>7. Reporting accuracy</p> <ul style="list-style-type: none"> <li>• Self-assessment</li> <li>• Data quality management</li> <li>• Reconciliation &amp; sign-off</li> <li>• Adjustments</li> <li>• Risk models &amp; approximations</li> <li>• Stress testing &amp;</li> </ul>
<p>8. Comprehensiveness</p> <ul style="list-style-type: none"> <li>• Reporting inventory</li> <li>• Risk coverage</li> <li>• Risk management context</li> <li>• Enterprise risk management</li> </ul>	<p>9. Clarity &amp; usefulness</p> <ul style="list-style-type: none"> <li>• Board reporting</li> <li>• Senior management reporting</li> <li>• Operational reporting</li> <li>• Risk MI framework</li> <li>• Risk data glossary</li> </ul>	<p>10. Frequency</p> <ul style="list-style-type: none"> <li>• Requirements definition</li> <li>• Regular reporting</li> <li>• On demand stress and crisis reporting</li> </ul>	<p>11. Distribution</p> <ul style="list-style-type: none"> <li>• Policies and procedures</li> <li>• Reporting mechanisms</li> <li>• Data security</li> </ul>



## Contacts



### **Johannes Grosskopf**

Banking Leader: PwC Africa  
+27 (0) 11 797 4346  
johannes.grosskopf@za.pwc.com



### **Costa Natsas**

FS Risk and Regulation Leader  
+27 (11) 797 4105  
costa.natsas@za.pwc.com



### **Tom Fish**

UK Risk Director, BCBS 239 Lead  
+44(0) 207 212 6341  
tom.f.fish@uk.pwc.com



### **Stephen Owuyo**

FS Risk and Regulation Specialist  
+27 (11) 797 4275  
stephen.x.owuyo@za.pwc.com

## Additional survey authors

**Adrian J Ellis**

**Nitin Chibba**

**Vinolin Naidoo**



© 2016 PricewaterhouseCoopers (“PwC”), a South African firm, PwC is part of the PricewaterhouseCoopers International Limited (“PwCIL”) network that consists of separate and independent legal entities that do not act as agents of PwCIL or any other member firm, nor is PwCIL or the separate firms responsible or liable for the acts or omissions of each other in any way. No portion of this document may be reproduced by any process without the written permission of PwC (16-18663)