Risk, data and the supervisor
The clock is ticking …
To start a new section, hold down the apple+shift keys and click to release this object and type the section title in the box below.
Resilience and transparency are driving a regulatory focus on data within G-SIBs, but the clock is ticking for all banks

This paper provides a Deloitte perspective on the recent Basel Committee on Banking Supervision (BCBS) consultative document ‘Principles for Effective Risk Data Aggregation and Risk Reporting’. We present a point of view on the regulatory drivers for change within the industry, the implications for banks and discuss the actions that should be undertaken over the coming months.

The BCBS proposes 14 principles to ensure that data and associated processes used by the risk function are “fit for purpose”. Global Systemically Important Banks (G-SIBs) are required to implement the principles in full by the beginning of 2016. However, they will need to submit a self-assessment against the principles to their local supervisor in 2013.

The BCBS paper sets clear expectations that banks will quantify their risk appetite and have robust infrastructure, processes and controls in place to monitor risks within the appropriate thresholds across credit, market, liquidity and operational risk. A summary of the 14 principles is provided in the table below.

### Summary of BCBS Principles for Effective Risk Data Aggregation and Risk Reporting

| Governance and Infrastructure | • The bank’s board and senior management must understand deficiencies in all aspects of the controls and aggregated data.  
|                              | • Organisational boundaries must be overcome so risk data can be accurately aggregated across business lines, jurisdictions and legal entities in a timely manner.  
|                              | • Systems must support risk data aggregation and reporting, including during times of stress or crisis. |
| Risk data aggregation capabilities | • Banks must demonstrate the ability to generate accurate and reliable aggregated risk data, largely automated to minimise errors.  
|                              | • The capabilities will also need to meet all on-demand and ad hoc reporting scenarios in a timely manner, including during crisis situations and in response to a supervisory request. |
| Risk reporting practices | • Banks must ensure that reconciled, validated and accurate risk reports are presented to the appropriate stakeholders in a timely manner to support the decision making process.  
|                              | • The reports must cover all material risk areas within the organisation and be easily understood by recipients.  
|                              | • All material gaps or weaknesses are well understood and factored into the decision making process. |
| Supervisory review, tools and cooperation | • Supervisors will review and monitor banks’ compliance with the principles and use appropriate tools to ensure deficiencies are addressed in an effective and timely manner.  
|                              | • The supervisor should have the ability to restrict growth in a bank’s risk-taking activities should it have concerns about data deficiencies. |

While the individual BCBS principles cover specific aspects of risk data management and reporting, it is clear the overall intent is to set a benchmark for what is acceptable in the way a bank manages and reports risk. The implications are wider than VARs or P&L strips and have major implications for a bank’s risk operating model and, more broadly, how data is managed across the bank.
Regulatory context

Moving data to centre stage

In the aftermath of the financial crisis, firms’ risk management processes came under increasing regulatory scrutiny. The focus of new legislation is expanding to encompass risk governance alongside more stringent technical requirements, particularly data. The aim of the data agenda is two-fold; firstly to rectify the perceived inadequacies of banks’ data capabilities during the financial crisis, particularly with regards to risk management. Secondly to ensure that firms can meet the ever growing data capture and reporting requirements that have sprung up as a result of initiatives aimed at improving the resilience and transparency of the financial system.

The ability of firms to provide timely, high quality and accurate data is a key international priority from both the perspective of macro-prudential surveillance and as an integral component in the effort to tackle the particular risks posed by Systemically Important Financial Institutions (SIFIs). Indeed inadequate data aggregation and insufficient risk reporting and IT systems have already been identified as an impediment to effective SIFI supervision. This has led to an influx of data focused international initiatives which have been endorsed at the G20 level, including the common data template for G-SIBs and the proposed BCBS principles for effective risk data aggregation and risk reporting discussed in this document. Data and data management are also a key focal point in the international work underway to increase transparency in the financial system through initiatives such as the legal entity identifier (LEI).

The issue of data has also moved to centre stage in both the EU and UK where there are a vast number of regulatory initiatives with a data reporting, processing and/or management element. These include the revisions to the Capital Requirements Directive (CRD 4) and the Capital Requirements Regulation (CRR), the proposal for revisions to the Markets in Financial Instruments Directive (MiFID II), European Market Infrastructure Regulation (EMIR) and Recovery and Resolution Directive (RRD) to name but a few. In addition there appears to be no sign of slowdown with new initiatives constantly emerging such as the Wheatley Review of LIBOR, which is likely to have a strong data element when recommendations are finalised. Furthermore, the European Supervisory Authorities (ESAs) and Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) in the UK will increasingly expect firms to extract and report specific risk data on demand.

Whilst sceptics of this revamped focus have argued that supervisors have often talked tough on data before and question their resolve to follow-through, on balance Deloitte believe this time it is quite different. Firms that put their head in the sand in the hope that this will all blow over could be in for a shock. It has already been made clear in regulatory papers and speeches that firms will be subject to supervisory reviews to ensure they are compliant with data requirements. Indeed the Bank of England and the Financial Services Authority (FSA) have stated that the new PRA will validate firms’ data “through onsite inspections.” In addition the proposed BCBS risk data principles, advocate testing firms’ data processes to ensure they are robust enough to withstand a range of adverse scenarios including a surge in business volumes and potential crisis situations. Furthermore, the BCBS suggests allowing supervisors to set limits on a firm’s ability to take on new risks or expand its business operations where deficiencies in data aggregation are considered to be serious enough to significantly impede risk management.

One thing is certain, poor quality, incomplete and inconsistent data is likely to put a serious strain on a firm’s relationship with its supervisors and will lead to further scrutiny and challenge of the sufficiency of its risk management and governance processes in general.

The table below shows the impact of regulatory requirements on data management processes.

<table>
<thead>
<tr>
<th>Regulatory initiative</th>
<th>Data capture</th>
<th>Data aggregation</th>
<th>Data reporting</th>
<th>Data protection</th>
<th>Data governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCBS principles for data aggregation and risk reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSB common data template for G-SIBs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Entity Identifier initiative</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCBS review of pillar 3 disclosure requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery and Resolution Directive (RRD)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revisions to Capital Requirements Directive (CRD 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Reporting (COREP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MiFID II</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>European Market Infrastructure Regulation (EMIR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revisions to the Market Abuse Directive (MAD II)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Commission proposals on reform of data protection rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEPA Regulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICB recommendations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Changes to the UK supervisory architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wheatley Review of LIBOR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Disclaimer**

Our impact analysis is based on policy measures proposed in the latest official text for each regulatory initiative which may be subject to change.

We have assumed as a starting point that banks’ data processes are adequate to meet current regulatory requirements. The actual impact will significantly vary from bank to bank.
Looking beyond the principles

To understand the implications of the BCBS paper the scope must be viewed through a risk lens and a data lens. Why? Because the data dimension and the risk dimension require separate and distinct solutions and pose two very different challenges.

‘Risk lens’

While it is obvious from the title that the BCBS paper is addressed to the risk function, what is not immediately evident is that the implications for risk’s operating model are far wider than data aggregation and reporting capabilities.

Notable requirements that will have significant implications for many banks include:

- A bank’s board and senior management should be fully aware of any limitations that prevent full risk data aggregation in terms of coverage (e.g. risks not captured or subsidiaries not included), in technical terms (e.g. risk model performance indicators or degree of reliance on manual processes) or in legal terms (e.g. sharing data across jurisdictions) (Para 23).

- The scope relates to all risks facing the bank including Credit, Market, Liquidity and Operational risk (Para 47). An example of time-critical operational risk is given as system unavailability or unauthorised access (Para 38 (e)).

- The ability to define risk appetite in a measurable way and then monitor Credit, Market and Operational risks against these tolerances is expected (Para 12). Following on from the above point, a measurable appetite for operational risk must be developed and tolerance levels set for the likes of system unavailability or unauthorised access risks.

- The group structure should not hinder aggregation capabilities at a consolidated level or any relevant level within the organisation (Para 22). Regional, legal entity or business line boundaries must be overcome to enable one group level view of risk consistent across geography and business units.

- Banks are expected to maintain documented processes for reconciling reports: automated and manual reasonableness checks including an inventory of the validation rules, procedures for identifying and explaining data errors and precision requirements for regular and crisis reports (Para 44 & 45).

While banks will recognise the importance of the 14 principles in establishing a robust risk management function, it is likely that many will not have this level of maturity in their current risk operating model.

‘Data lens’

The focus of the BCBS paper is on risk data but the implications are far wider than P&L strips or VAR metrics. The old adage of ‘rubbish in, rubbish out’ is a universal truth and implicit in the BCBS’s principles is that underlying data which enables the generation of risk metrics must also be of sufficient quality. This means all forms of reference and transaction data consumed by the risk function fall within the scope of the principles. This includes counterparty data, legal entity hierarchies, book data, trade data, prices, instrument static etc.

The implications of this are huge. While the risk function is clearly responsible for the data it generates and aggregates, it is not responsible for reference or transaction data it consumes. Initial analysis of the BCBS paper may lead organisations to conclude they require a risk-data management solution. However, the requirement is much broader - an organisation-wide solution is required that will own and resolve reference or transaction data issues that affect the risk function.

While many banks have some form of data management function, Deloitte’s experience is that banks have focussed on tactical work-arounds (such as manual adjustments and off-system data analysis) and not taken a more strategic approach to data management. The BCBS paper strengthens the business case for strategic change rather than yet another quick fix. For those in banks today who are trying to get the data problem recognised at CxO level and secure budget and support to improve the effectiveness of the data management function, the BCBS paper significantly strengthens the business case for change.

In many respects, the risk dimension may be an easier challenge to address as there is a defined risk organisation and operating model which reports into an accountable executive – the Chief Risk Officer. The data dimension is different. The majority of reference or transaction data in a bank is shared across many different functions and lacks a single accountable owner making it very difficult to make the necessary changes across people, process and technology.

Who should lead this data management function within the bank? This is a common challenge for many banks that are starting to tackle the data question and there is no easy answer. The role of Chief Data Officer is becoming more common but many banks still look to the CIO or CTO because data is still viewed as an ‘IT issue’. However, Deloitte’s experience shows that ‘business-side’ executives must take the lead, starting with a Data Governance committee comprising of senior executives from across the functions (Operations, Risk, Finance, Sales & Trading etc) with the authority and willingness to drive change in their own organisations for the greater good of the firm.
What needs to be done now?

The clock is ticking; supervisors will be expecting G-SIBs to begin self-assessment preparation now

In preparing the self-assessment submission, banks may be tempted to only focus on satisfying each individual principle. However, while it is important to identify data issues within the self-assessment, it is critical to demonstrate to the supervisor a deep understanding of the current operating model and its deficiencies, alongside a strategic level of commitment to reach the required level of maturity and a robust plan to get there.

Timeline
G-SIBs will be subject to external monitoring of their implementation of, and ongoing compliance with, the principles outlined in the BCBS paper. Supervisors across all relevant jurisdictions will be responsible for establishing a programme of ongoing review, through both firm-specific reviews and broader industry-wide thematic reviews.

It is expected that national supervisors will start discussing the principles with G-SIBs in early 2013, ahead of a self-assessment submission later in the year. By 2016 all G-SIBs should have addressed the principles and closed any significant gaps.

An overview of the timeline to the 2016 deadline is shown below.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
<td>Q4</td>
<td></td>
</tr>
</tbody>
</table>

**BCBS consultative document**
- Self-assessment of:
  - Maturity of governance model
  - Adequacy of data/IT design
  - Group-wide data gap analysis (assess accuracy, completeness, timeliness, adaptability)
  - Adequacy of management reporting

**Self-assess against principles**

**Supervisors to discuss with G-SIBs**
National supervisors to discuss implementation of the principles with senior management in early 2013

**Define strategy to address gaps**
G-SIBs to define strategy for addressing gaps between self assessment and proposed risk aggregation framework

**Establish and deliver initiatives**

**BCBS tracking via SIG**
Tracking via Standards Implementation Group (SIG)

**Status to be shared with FSB**
BCBS to share findings with FSB at least annually

**Deadline for meeting expectations and implementing principles**
All principles to be addressed and significant gaps closed

G-SIB Actions/Milestone  Supervisory Actions/Milestone
**Activities**

A self-assessment framework must be developed that incorporates the 14 principles. The framework should be developed by the risk function and owned by the Chief Risk Officer and embedded in the group’s operating model so that the framework becomes part of business-as-usual rather than a tool for responding to a supervisory request.

One of the first activities of the self-assessment should define what ‘fit for purpose’ risk data looks like. The next step is to undertake a data quality review to determine reference and transaction data deficiencies as soon as possible. These data deficiencies must be passed onto the bank’s data management function for effective and timely resolution.

The table below outlines the suggested activities required to prepare for the self-assessment submission.

<table>
<thead>
<tr>
<th>Suggested activities to prepare for the self-assessment submission</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk</strong></td>
</tr>
<tr>
<td>1. Assign an Executive who will take ownership and be accountable to the Chief Risk Officer for delivery against the BCBS requirements.</td>
</tr>
<tr>
<td>2. Assemble a steering committee comprising appropriate senior stakeholders with responsibility across global risk i.e., regional and legal entities coverage.</td>
</tr>
<tr>
<td>3. Define the self-assessment framework;</td>
</tr>
<tr>
<td>a) develop the set of questions, weightings and associated thresholds that will enable qualitative and quantitative evaluation against each principle;</td>
</tr>
<tr>
<td>b) design and build a tool to capture and report the self-assessment responses;</td>
</tr>
<tr>
<td>c) define the self-assessment execution plan and identify relevant departmental owners.</td>
</tr>
<tr>
<td>4. Undertake an initial self-assessment, identifying areas for further investigation and prioritising gaps for remediation.</td>
</tr>
<tr>
<td>5. Establish initiatives to deliver remediation activities.</td>
</tr>
<tr>
<td>6. Embed the self-assessment approach within the business as usual processes.</td>
</tr>
<tr>
<td><strong>Data</strong></td>
</tr>
<tr>
<td>1. Critically assess the capabilities of the data management function to meet the needs of the risk initiatives.</td>
</tr>
<tr>
<td>2. On the assumption that aspects of the data management function will be deficient</td>
</tr>
<tr>
<td>a) escalate the issue to board level; appoint an accountable executive (typically Chief Data Officer) and establish a group level data management committee comprising of executive level stakeholders from business and IT;</td>
</tr>
<tr>
<td>b) define and establish an effective data management function across the group;</td>
</tr>
<tr>
<td>c) assemble a delivery team who are able to deliver change across people, process and technology.</td>
</tr>
<tr>
<td>3. Formally accept risk data issues and agree delivery timeline with risk.</td>
</tr>
</tbody>
</table>

Although the self-assessment framework will be owned by the risk function, there are number of other stakeholders that should be consulted as part of this process, such as compliance and internal audit. Compliance will need to determine the nature of their involvement regarding the self-assessment submission to the supervisor.
Conclusion

G-SIBs need to act now to meet the 2013 deadline but those that embrace this opportunity to deliver strategic change will gain competitive advantage.

It is clear that the ‘eye’ of the supervisory community is moving onto data management and away from simply prescribing the data outputs; and given the focus of the supervisory community on systemic risk, it is no surprise that risk data is under increased scrutiny.

Ensuring effective and accurate risk data aggregation across all business lines, jurisdictions and legal entities will be a major challenge for those banks that have multiple risk operating models, of varying maturity levels, and a technology and data landscape that is disparate and siloed. Establishing a data management function that can address the organisational, process and technology layers of the data lifecycle across front-office and operations, as well as other functional areas, is a goal that many have tried to achieve but with little success.

G-SIBs need to act now to be ready for self-assessment in 2013; however, all banks should recognise this paper as a sign of things to come and start to assess the current maturity of their risk operating model and data management function and develop a plan to move up the curve.

This is also an opportunity to differentiate the bank in the eyes of investors through an industry-leading risk function, to optimise regulatory capital, to establish a data management function that can increase revenue through client insights, differentiate services, improve STP rates, and decrease costs across the bank. In short, this is an opportunity to gain sustainable competitive advantage.
**Deloitte Spain contacts**

Francisco Celma  
*Partner – Financial Services Leader*  
Deloitte S.L.  
+34 91 443 27 47  
fcelma@deloitte.es

Miguel Ángel Bailón  
*Partner – Financial Services*  
Deloitte S.L.  
+34 91 438 17 34  
mbaillon@deloitte.es

Francisco Ambros  
*Partner – Financial Services*  
Deloitte S.L.  
+34 93 253 37 44  
iambros@deloitte.es

**Contacts**

Steve Swain  
*Partner – Financial Services*  
Deloitte MCS Limited  
020 7007 4255  
steveswain@deloitte.co.uk

Tom Scampion  
*Partner – Data Analytics*  
Deloitte LLP  
020 7007 2828  
tscampion@deloitte.co.uk

David Strachan  
*Co-Head of Centre for Regulatory Strategy*  
Deloitte LLP  
020 7303 4791  
dastrachan@deloitte.co.uk

Paul Garel-Jones  
*Director – Data Analytics*  
Deloitte LLP  
020 7303 3069  
pjgareljones@deloitte.co.uk

Adrian Walsh  
*Senior Manager - Financial Services*  
Deloitte MCS Limited  
020 7303 2441  
awalshe@deloitte.co.uk

**Related Deloitte publications**

**Aggregated risk on demand: Why shareholders need what regulators want**

This paper explains how developments in the scale and speed of computing are enabling a new technology known as ‘aggregated risk on demand’. We detail how it can help firms drive up returns on equity by improving their pricing, optimising their portfolios, conserving capital, cutting costs and enabling smarter, more timely decisions.

**Growth, risk and compliance – Taking a strategic approach to managing reference data**

Co-authored by Deloitte and SWIFT and with contributions from Chief Data Officers across the industry, this paper outlines the pervasive impact that poor reference data can have on organisations and makes the case for a strategic approach to managing reference data.

These publications are available on the Deloitte UK website:

To start a new section, hold down the apple+shift keys and click to release this object and type the section title in the box below.