Principles for effective Risk Data Aggregation and Risk Reporting

Jonathan Van Malleghem
Senior Consultant
Avantage Reply

Frederic Blard
Senior Consultant
Avantage Reply

In January 2013, the Basel Committee on Banking Supervision ("BCBS") issued a set of Principles ("the Principles") to improve banks' risk management practices, decision-making processes and resolvability. Firms designated as global systemically important banks ("G-SIBs") are required to implement the Principles in full by the beginning of 2016.

Like the BCBS, national regulators believe that the Principles can be applied to a wider range of banks. This Practice Note looks into the implementation of the Principles to date not only in G-SIBs but also in medium-sized banks.

Background

"One of the most significant lessons learned from the global financial crisis that began in 2007 was that banks' information technology ("IT") and data architectures were inadequate to support the broad management of financial risks."[1]

In response, the Basel Committee—as well as other global regulatory standard setters and national regulators—introduced a range of requirements to strengthen banks' risk data aggregation capabilities and risk reporting practices.

Whilst most banks have projects in place to enhance existing 'reporting chains', the Principles established a high standard and further work is still required to achieve compliance with the exacting BCBS standards by 2016.

> "Many banks are facing difficulties in establishing strong data aggregation governance, architecture and processes, which are the initial stage of implementation. Instead they resort to extensive manual workarounds which are likely to impair risk data aggregation and reporting."
>
> Basel Committee on Banking Supervision
> December 2013

Within this Practice Note, we present our recommended approach to overcoming certain practical challenges. We draw on our recent experience with some of the G-SIBs as well as a few large domestic banks with whom we enjoy the privilege of working.

Introduction to the Principles for Effective Risk Data Aggregation and Risk Reporting

As noted above, the Principles are expected to be implemented by G-SIBs by January 2016. The BCBS also recommends that national supervisors extend their application to domestic systemically important banks ("D-SIBs"). We, at Avantage Reply, believe the Principles will receive wide adoption and will eventually impact most banks in the European Union ("EU").

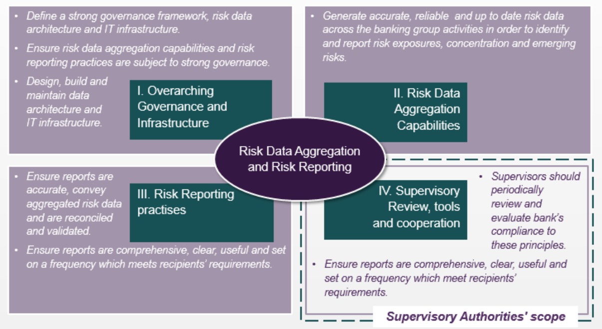
The principles cover four closely related topics:

- Overarching governance and infrastructure;
- Risk data aggregation capabilities;
- Risk reporting practices; and

[1] Principles for effective risk data aggregation and risk reporting, BCBS, January 2013, page 1.

- Supervisory review, tools and cooperation.

These are then broken down into a total of 14 principles.



Based on our observations to date, and assuming a pragmatic approach is adopted, the changes ensuing from the implementation of the Principles are likely to create value. They lead to improved decision-making information being provided to senior management in a more timely and cost efficient manner. In turn, this improves the decision-making process at Group level within the financial institution and across legal entities.

G-SIBs' Self-Assessment and Implementation Challenges

Following the issuance of the Principles, the Basel Committee developed a questionnaire (87 questions/requirements for 11 principles), the results were subsequently analysedand several recommendations were set out for 2014 to ensure that banks are able to meet the 2016 deadline. The main results of the exercise are highlighted in the chart below:

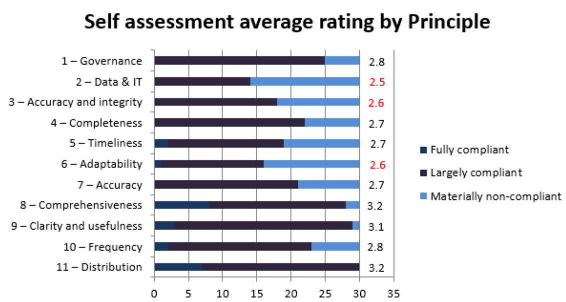


Figure 1: Self Assessment Ratings by Principles (adapted from BCBS, December 2013)

As depicted in Figure 1, the average ratings of Principles 1 to 11 ranged from 2.5 to 3.2. The average rating of all 11 Principles was 2.8, which indicates that the banks' average reported compliance status ranges between largely compliant and materially non-compliant.

It is noted that the three principles with the lowest reported compliance were Principle 2 (data architecture/IT infrastructure), Principle 6 (adaptability) and Principle 3 (accuracy/integrity); hence our focus on those in the following sections.

Addressing BCBS 239: Avantage Reply's recommended approach

Principle 2: Data Architecture and IT Infrastructure

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

The average rating for this Principle (2.5) was the lowest rating of the 11 Principles. Data architecture and IT infrastructure would appear to be two of the most critical and challenging issues for banks.

In our view, Principle 2 is critical to the wider risk management framework; compliance with the Principles and producing reliable and timely risk data and reports can only be achieved with robust data architecture and IT infrastructure.

The data architecture and IT infrastructure should be such that risk data aggregation capabilities and risk reporting practices are sufficiently robust and flexible enough to address their potential needs in normal times, as well asduring times of stress/crisis. Banks generally agree that enhancements are still needed regarding their capabilities to address MI requirements during normal times. Most banks concede that they experience significant challenges in producing the MI required during times of stress. The Asset Quality Review ("AQR") exercise, led by the European Central Bank and the European Banking Authority ("EBA"), and the ECB stress test exercise are two recent examples demonstrating the difficulty faced by banks when they are requested to provide additional ad-hoc information and data by regulators.

Another example relates to inconsistencies between regualtory reports (e.g., COREP and FINREP) prepared by banks. These reports, which source (inconsistent) data from Risk and Finance systems, remain, in some institutions, an ongoing challenge that can only be avoided with a consistent, clear and complete data architecture and IT infrastructure.

Often, banks have difficulties in harmonising the different reporting chains and ensuring a comprehensive group-wide standardisation of integrated data taxonomies and architecture.

A pre-requisisite to meet these requirements is to enhance the transparency (i.e. the bank's understanding) of key risk data elements as they 'flow across the risk architecture'. Once that data inventory and its flows starts to emerge, one can then overlay this view with the appropriate governance & control framework.

We have observed how the recommended approach ,albeit conceptually simple, can truly change the understanding of a bank's risk data and IT infrastructure. Through an improved understanding of the 'as-is', governance & control structures will become more effective and the level of alignment and 're-use' can be drastically improved with a leaner and more compliant data landscape as a result.

By collaboratively building an understanding of their data within their Business context using tools such as Axon™, banks can pave the way towards sustained compliance with Principle 2.

Principle 3: Accuracy and Integrity

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

The average rating for this Principle was 2.6, which was the third lowest score among the 11 Principles.

Accuracy and integrity are the essence of reporting and banking as a whole. However, the perfect balance between timeliness, cost and accuracy is not easy to strike. The Principle states that a bank should be able to generate accurate and reliable risk data under normal conditions as well as under stress conditions.

One of the BCBS's primary recommendations is to minimise the probability of errors by utilising an automated reporting chain. BCBS acknowedges that manual interventions within the reporting chain are warranted where judgement is required. However, regulators are increasingly wary of high levels of dependency on manual processes that pose a challenge to accurate and timely risk data aggregation.

In order to reduce the probability of errors due to manual interventions, first, an assessment of the current processes must be made. Secondly , the unnecessary manual interventions must be removed. As a last step, the remaining manual interventions must be documented and automatic controls should be implemented where possible to mitigate operational risk.

A second area of focus should be the different shortcuts or so-called 'defaulting' applied within the reporting chain. Going from the front office systems to the final figures, data undergoes different transformations. These should be clearly documented and banks should assess whether these transformations can be avoided. This is particularly important when it comes to ad-hoc risk data reporting (as is the case under a stress scenario).

Principle 6: Adaptability

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

Adaptability is one of the most important challenges faced by large financial institutions. Regulators expect a banks risk data aggregation capabilities to be flexible and adaptable to meet ad-hoc data requests as needed, and to be capable of assessing emerging risks. For example, they expect banks to be able to generate subsets of data based on requested scenarios or resulting from economic events (e.g. as was the case during the recent EBA and ECB exercises).

The main solution to enable such requests is to have a uniform and standardised reporting chain. As discussed above, Principle 2, *Data Architecture and IT Infrastructure*, is the essence of the BCBS's general requirement.

Unfortunately, even if there was universal agreement that implementing such a data architecture would be useful (also for internal requests), the implementation is time intensive and therefore a three-year timeframe may not be adequate.

Until such an architecture is in place, however, quick wins can be identified. For example, tracing back risk data through the chain and integrating the essential data in one user-friendly data warehouse which can provide quick ad-hoc reports based on user requirements (group-wide, business unit view, legal entity view, etc.), proved very useful to a G-SIB when addressing ad-hoc regulatory demands.

June 2014

.

Contacts

Avantage Reply (Belgium)
Jonathan Van Malleghem
Senior Consultant
Avantage Reply
5 Rue du Congrès | 1000 Brussels | Belgium
Tel: +32 2 880 03 24
E-mail: j.vanmalleghem@reply.eu

Avantage Reply (Luxembourg)
Frederic Blard
Senior Consultant
Avantage Reply
46a, avenue J.F. Kennedy | 1855 Luxembourg | Luxembourg
Tel: +352 26 005 264
E-mail: f.blard@reply.eu

Avantage Reply (France)
Frederic Blard
Senior Consultant
Avantage Reply
5, rue des Colonnes – 6th floor | 75002 Paris | France
Tel: +33 1 47 03 92 90
E-mail: f.blard@reply.eu

Avantage Reply (The Netherlands)
Arnold Veldhoen
Associate Partner
Avantage Reply
3rd Floor, The Atrium | Strawinskylaan 3051 | 1077 ZX Amsterdam | The Netherlands
Tel: +31 (0) 20 301 2123
E-mail: a.veldhoen@reply.eu

Avantage Reply (Italy)
Maria Scarcella
Partner
Avantage Reply
Via Castellanza, 11 | 20151 Milan | Italy
Tel: +39 02 535761
E-mail: m.scarcella@reply.eu

Xuccess Reply (Germany)
Rainer Geckeler
Partner
Xuccess Reply
Arnulfstr. 27 | D-80335 München | Germany
Tel: +49 (89) 411142-200
E-mail: R.Geckeler@reply.de