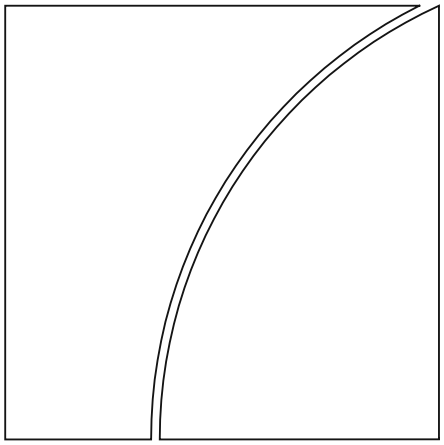
Basel Committee
on Banking Supervision



Progress in adopting the Principles for effective risk data aggregation and risk reporting

June 2018

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9197-484-9 (online)

Contents

Progress in adopting the Principles for effective risk data aggregation and risk reporting

Executive summary

Banks have found it challenging to comply with the Principles, due mainly to the complexity and interdependence of IT improvement projects. As a result, the expected date of compliance has slipped back for many banks. The 2017 assessment showed that most banks had made, at best, marginal progress in their implementation of the Principles. Even though the implementation deadline of 1 January 2016 has passed, only three G-SIBs have been assessed by their supervisors as achieving full compliance with all Principles. The lengthening of the G-SIBs' expected time line to achieve full compliance with the Principles can be attributed in part to (i) the dynamic nature of complying with the Principles, (ii) underestimation of efforts needed to fully comply with the Principles, including the time needed to address IT legacy issues; and (iii) higher supervisory expectations as a result of the additional supervisory activities conducted to assess banks' implementation of the Principles.

Banks have developed implementation roadmaps that focus mainly on addressing issues related to governance, data quality and IT infrastructure. Banks should remain committed to their initiatives for implementing the Principles and avoid further deadline slippages. Banks should take concrete actions and continue to make progress in the implementation of the Principles according to the roadmaps agreed with their supervisors. As the compliance deadline has already passed, further delays should be avoided.

Banks should consider how implementation of the Principles would benefit other initiatives. As banks implement the Principles in relation to their internal risk reporting processes, they are encouraged to consider how the upgrades on their risk data aggregation and risk reporting (RDARR) practices will allow them to comply more effectively with other initiatives and requirements relating to data (eg recovery and resolution plans).

1. Introduction

The Basel Committee published the Principles in January 2013 with the aim of strengthening banks' risk data aggregation capabilities and internal risk reporting practices.[1] Since the publication of this framework, the Basel Committee has been monitoring banks' implementation.

The Risk Data Network (RDN)[2] established under the Committee's Supervision and Implementation Group (SIG) has been monitoring implementation of the Principles, which went into effect in January 2016. Although assessing banks' ability to comply with the principles-based framework is challenging, the Committee made an explicit decision not to prescribe any objective or quantitative benchmarks for judging compliance with it. This approach acknowledges that risk management and risk

1 BCBS, *Principles for effective risk data aggregation and risk reporting*, January 2013, www.bis.org/publ/bcbs239.pdf.

2 Formerly known as the Working Group on SIB Supervision (WGSS). In early 2016, the WGSS was transformed into the RDN. The RDN's mandate is similar to that of the WGSS, which is to carry on the monitoring work for risk data, but with a stronger focus on supervisory evaluations. The RDN adopts an evidence-based approach to monitoring, and reports to the SIG in respect of compliance levels and evidence of good practices among banks. RDN members meet and exchange information on implementation strategies and supervisory approaches to further implementation of the Principles.

data aggregation practices vary considerably across banks, depending on their business models, structure and/or risk profiles.

In 2013–15, the Committee published three reports based on banks' self-assessments of their progress towards compliance with the Principles.

In March 2017, the RDN published a progress report on G-SIBs' progress in implementing the Principles during the previous year. These observations were based on the results of an assessment survey completed by authorities with supervisory responsibility for G-SIBs.[3] The report highlights that, while some progress has been made, most G-SIBs have not fully implemented the Principles and the degree of compliance is unsatisfactory. In view of these results and to promote further adoption of the Principles, the recommendations set out within the report include:

- Banks should develop clear roadmaps to achieve full compliance with the Principles and comply with them on an ongoing basis.
- Supervisors should: (i) communicate their supervisory assessments with the banks and provide the necessary incentives for full compliance with the Principles; and (ii) continue to refine their approaches to assessing banks' compliance.

Given the unsatisfactory degree of implementation, the Committee conducted another monitoring exercise in 2017. As in the 2016 assessment, supervisors were asked to complete a survey to assess their banks' progress towards compliance with the Principles. The 2017 version of the survey focused more on the reasons for banks failing to achieve full compliance with Principles 1 and 2, which are the preconditions for complying with the remaining principles. The supervisory assessments form the basis for this report.

The aim of this report is to assess banks' implementation of the Principles, identify key deficiencies and propose key recommendations to promote implementation. Section 1 summarises the work conducted to date. Section 2 gives an overview of how far banks are in compliance with the Principles, including the key observations of supervisors regarding the main deficiencies in banks' current implementation strategies. Section 3 discusses implementation by domestic systemically important banks' (D-SIBs). Section 4 proposes recommendations for banks and supervisors in the near to medium term. In addition, Appendix 2 contains supervisors' detailed assessments of compliance with the Principles and examples of effective implementation practices observed in recent assessment exercises.

2. Assessment results and key observations

The 2017 assessment was completed by all seven supervisors/supervisory regimes with G-SIBs in their remit. The 2017 assessment covered 30 banks designated as G-SIBs in 2011 or 2012 and subject to the January 2016 implementation deadline (henceforth referred to as "banks").[4]

2.1 Overview of assessment results in 2017

As in the 2016 exercise, supervisors were asked to rate their banks' current degree of compliance with each of the RDARR Principles on a 1 to 4 scale. The four ratings were defined as follows:

[3] Progress reports published prior to the progress report for the 2016 assessment were based on banks' self-assessment. The 2016 and 2017 assessments are based on supervisors' assessments.

[4] G-SIBs designated in subsequent annual updates will need to comply with the Principles within three years of their designation.

- Rating of "4" – *The Principle is fully complied with*: The objective of the Principle is fully achieved with the existing architecture and processes;
- Rating of "3" – *The Principle is largely complied with*: Only minor actions are needed in order to fully comply with the Principle;
- Rating of "2" – *The Principle is materially non-compliant*: Significant actions are needed in order to progress further or achieve full compliance with the Principle; and
- Rating of "1" – *The Principle has not been implemented*.

In addition to the ratings, supervisors provided qualitative inputs in the assessment survey. For instance, supervisors were asked to comment on the key advances made by their supervised banks in the implementation of the Principles since the 2016 assessment.

Overall, most banks had made, at best, marginal progress in their implementation of the Principles, which is unsatisfactory. It is clear that banks will require more time than previously indicated to achieve full compliance with the Principles. However, looking beyond the quantitative results, banks have accelerated their efforts and taken positive action to comply with the Principles.

2.1.1 Levels of compliance

Graph 1 and Table 1 show, respectively, the banks' degrees of compliance and their average compliance ratings. No principle is fully complied with by all banks. Looking at the individual principles, there were no changes in compliance ratings which were greater (in either direction) than 0.13. Within the set of principles, Principle 1 (Governance) and Principle 2 (Data architecture and IT infrastructure) are of the utmost importance. These two principles have been designated as preconditions, in that banks need to have in place a strong governance framework, risk data architecture and IT infrastructure to ensure compliance with the remaining principles (ie Principles 3 to 11). The insufficient improvement in the average compliance ratings for Principle 1 (from 2.83 in 2016 to 2.90 in 2017) and Principle 2 (from 2.60 in 2016 to 2.73 in 2017) partially explains the minimal progress observed in the average ratings for the other principles.

It should, however, be noted that the performances of individual banks could be masked by averaging effects – for instance, the fact that one bank made good progress in implementing the Principles in 2017 does not show up in the average ratings. The bank complied fully with four principles in 2017, as compared with none of the principles in 2016.

Graph 1 – Levels of compliance by Principle

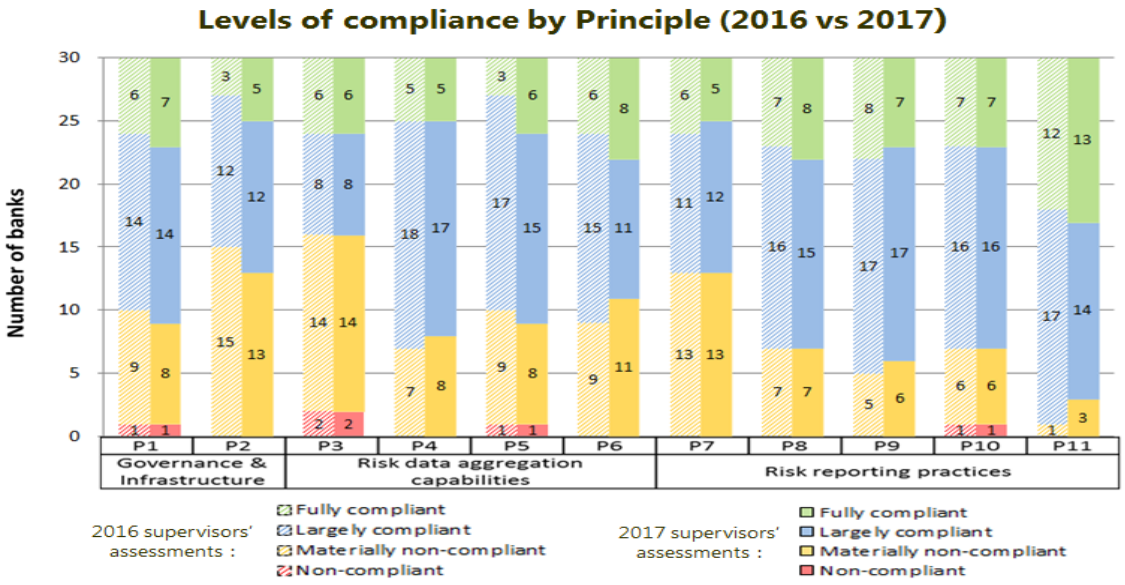


Table 1 – Average compliance ratings of banks, 2016 and 2017[5]

Assessments	Governance & infrastructure		Risk data aggregation capabilities				Risk reporting practices				
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
2017	2.90	2.73	2.60	2.90	2.87	2.90	2.73	3.03	3.03	2.97	3.33
2016	2.83	2.60	2.60	2.93	2.73	2.90	2.77	3.00	3.10	2.97	3.37
Differential	0.07	0.13	0.00	-0.03	0.13	0.00	-0.03	0.03	-0.07	0.00	-0.03

2.1.2 Expected date of compliance

Table 2 shows the dates by which the supervisors expect the banks to comply fully with the Principles as at end-2017. Even though the implementation deadline of 1 January 2016 has passed, only three banks have been assessed by their supervisors as achieving full compliance with all Principles – far fewer than the 11 banks that were expected to be in full compliance by this time, as indicated in the 2016 assessment.

The lengthening of the banks' expected time line to achieve full compliance with the Principles can be attributed in part to (i) the dynamic nature of complying with the Principles; (ii) underestimation of efforts needed to fully comply with the Principles, including the time needed to address IT legacy issues, as well as the complexity and interdependence of IT improvement projects; and (iii) higher supervisory expectations as a result of the additional supervisory activities conducted to assess banks' implementation of the Principles.

As recommended in the progress report for the 2016 assessment, compliance with the Principles should be an ongoing process. Banks should reassess their compliance whenever there are any key changes in their business models and risk profiles as well as new strategic initiatives (eg mergers and acquisitions) which are likely to bring about new implementation challenges. For instance, some banks have discovered that the hurdles to achieving full compliance with the Principles have become higher as the Principles were implemented across the banking group (see Section 2.2.2).

Some banks have underestimated the efforts needed to fulfil the Principles, in particular, to address and update legacy IT systems. In some cases banks have not shown the commitment needed to meet project deadlines.

In some cases, the lengthening of the time line should also be set against the backdrop of higher supervisory expectations. Some supervisors have asked the banks to extend the coverage of their implementation of the Principles, as the initial scope was deemed to be unsatisfactory.

[5] Changes in the 2016 average compliance ratings of banks from the progress report for the 2016 assessment are due to adjustments made by a supervisor subsequent to the publication of the report.

Table 2 – Expected date of full compliance with all Principles

Full compliance by	Number of banks	
	2016	2017
End 2016	2	1
End 2017	9	2
End 2018	15	14
Beyond end 2018	4	13
Total	30	30

2.2. Key observations

The quantitative results should be interpreted with care. There are limits to how far quantitative ratings can reflect possible improvements. Improvements made by the banks in implementing the Principles may not show up immediately in the results as data architecture and IT system enhancements tend to be multi-year projects and supervisors need to assess that the improvements have indeed been made.

The qualitative responses of the supervisors show that banks have made efforts to implement the Principles, while uncovering more implementation challenges. At the same time, supervisors have increased their efforts to more intensively monitor banks' implementation activities.

2.2.1. Efforts made by banks to implement the Principles

Banks have increasingly recognised the value of implementing the Principles and have stepped up their efforts to do so. All banks now have in place implementation roadmaps assessed by their supervisors, in line with the recommendation in the progress report for the 2016 assessment that, by June 2017, banks should provide their national supervisors with clear roadmaps detailing how they intend to move towards full compliance with the Principles.[6]

In addition, some of the banks have taken one or more of the following steps to facilitate the implementation of the Principles:

- Continued/increased resource commitments to implementation and greater clarity on the resources to be committed. For instance, banks have committed funding specifically for the enhancement of IT systems and data architecture and made dedicated appointments such as Chief Data Officers.
- Improved capabilities in automating the production of risk data. For instance, enhancing the use of integrated data taxonomies and dictionaries and providing data lineage to a common pool of key data facilitates the automation of risk report production.

[6] The progress report for the 2016 assessment set out that a roadmap should minimally include:

- a time line for closing compliance gaps, with expected deliverables and mitigants or controls for deficiencies observed by supervisors;
- dedicated resources and oversight from board and senior management (eg putting in place a framework for management oversight on implementation progress) as a demonstration of the bank's commitment towards full compliance with the Principles; and
- tangible measures to demonstrate that implementation progress is being made.

- Enhanced compliance control frameworks and internal certification approaches. For instance, banks have set up self-assessment units to measure progress in compliance, and internal audit/compliance functions have independently validated the bank's compliance with the Principles.

2.2.2. Challenges faced by banks

The key challenges faced by banks in the 2016 assessment remain relevant.[7] In particular, banks continue to experience difficulties in implementing the Principles across an entire banking group and in managing the interdependencies between RDARR programmes and other bank-wide strategic projects.

The international scale of G-SIBs' operations creates challenges in ensuring consistent implementation across the banking group at all functional levels and in all material entities. For instance, some banks found that the varying processes and standards within significant subsidiaries hindered full compliance by the entire banking group. In certain cases, the IT systems and architecture of some of a banking group's overseas entities could not be fully integrated with those of the banking group without major system enhancements as they have to comply with local regulatory requirements.

In addition, as G-SIBs tend to have other bank-wide projects running alongside their RDARR programmes, the interdependencies between these projects may complicate their implementation of the Principles. For instance, implementation of the RDARR framework may depend on the finalisation of other data-related frameworks such as the group-wide risk management framework, as the Principles need to be applied in the same way to these other bank-wide projects.

Challenges specific to Principles 1 and 2

Given the importance of Principles 1 and 2 in enabling a bank's implementation of the remaining principles, the 2017 exercise investigated the reasons why banks are currently unable to achieve full compliance with these two principles.

Principle 1 requires a bank's group RDARR framework to be reviewed and approved by a bank's board and senior management. However, at some banks, the RDARR frameworks had not been appropriately approved. Principle 1 also requires that a bank's senior management be fully aware of and understand the limitations that prevent full risk data aggregation.[8] In this regard, it was observed that, for some banks, senior management had not been sufficiently informed of limitations in the bank's RDARR capabilities (eg an inappropriately narrow scope in risk data implementation projects, fragmented validation practices) or the challenges involved in sustainable data governance and management.

Principle 2 requires a bank to design, build and maintain a data architecture and IT infrastructure that fully support its risk data aggregation capabilities and risk reporting practices not only in normal times

[7] The progress report for the 2016 assessment highlighted that banks faced challenges in the form of technical issues and defining and assessing materiality. Major technical challenges faced by banks include:

- difficulties in execution and management of complex and large-scale IT and data infrastructure projects, such as resources and funding issues, deficiencies in project management and coordination with other ongoing strategic programmes;
- overreliance on manual processes and interventions to produce risk reports, though some manual processes are unavoidable;
- incomplete integration and implementation of bank-wide data architecture and frameworks (eg data taxonomies, data dictionaries, risk data policies); and
- weaknesses in data quality controls (eg reconciliation, validation checks, data quality standards).

[8] The senior management's understanding should be in terms of coverage (eg risks not captured or subsidiaries not included), in technical terms (eg model performance indicators or degree of reliance on manual processes) or in legal terms (legal impediments to data-sharing across jurisdictions).

but also during times of stress or crisis. In setting up the data architecture, the bank should also establish integrated data taxonomies and architecture across the banking group.[9] However, some banks are unable to comply fully with this Principle because they are still in the process of upgrading the data architecture for the banking group or material subsidiaries. In addition, it is noted that the data architecture and IT infrastructure of some banks struggle to meet the demands of their daily business operations, casting doubts on their risk reporting capabilities during times of stress. This is often linked to overreliance on manual processes, which places significant burdens on the middle office to prepare data, resulting in reporting inaccuracies.

2.2.3. Definition of materiality

The concept of materiality within the Principles means that banks can exceptionally exclude certain information from data aggregation and reporting (and in turn the application of the Principles), provided that such an exclusion does not affect a bank's decision-making processes.

The 2016 assessment showed that banks are struggling to define materiality thresholds that are acceptable to supervisors. Supervisors, understandably, have not prescribed materiality thresholds for the banks, as the concept of materiality is unique to each bank's business model and risk exposure. In this regard, the RDN sought to better understand how banks define materiality.

The 2017 assessment found that common factors used by banks in determining materiality thresholds include:

- Data and information from in-scope critical risk reports identified by bank management;
- Materiality definitions based on proportion of risk-weighted assets; and
- Material risks to which the banking group is exposed, as identified by the group's internal capital adequacy assessment process (ICAAP).

2.2.4. Increased supervisory intensity pertaining to banks' implementation of the Principles

In assessing banks' implementation against the commitments set out in the roadmaps, supervisors have applied a range of assessment techniques (eg thematic examinations, fire drills) which focus on banks' implementation of the Principles. In particular, some supervisors have increased their emphasis on conducting on-site supervision to assess banks' implementation of the Principles. Some supervisors report that inputs provided by banks during off-site reviews and the observations made during on-site inspections could be surprisingly different. Beyond ad hoc assessment exercises, some supervisors have also further integrated the assessment of banks' compliance with the Principles into their regular supervisory reviews (eg supervisory rating systems).

Increased supervisory efforts have enabled supervisors to assess the adequacy of the banks' implementation roadmaps and identify areas of weaknesses. The communication of supervisory expectations (via supervisory letters, frameworks setting out roles and responsibilities of board and senior management), has translated into more affirmative actions taken by banks in the implementation of the Principles. Some supervisors have raised their concerns with the banks about the slow implementation progress after the deadline of 2016 and informed them that their compliance with the Principles will be factored into the overall supervisory review and hence could potentially result in a higher Pillar II capital add-on.

[9] This includes information on data characteristics, as well as the use of single identifiers and/or unified naming conventions for data including legal entities, counterparties, customers and accounts.

3. Monitoring D-SIBs' implementation

In 2018, the RDN conducted a workshop for supervisors to exchange views on the implementation of the Principles for D-SIBs in their jurisdictions.

In general, the Principles are sufficiently flexible to be applied to D-SIBs. This accords with the aims of a principles-based framework which acknowledges that risk management and risk data aggregation practices may vary considerably across banks, due to differences in business models, structure and/or risk profiles.

On first sight, D-SIBs have made some progress in implementing the Principles.[10] In doing so, they seem to meeting the same challenges as those faced by G-SIBs, such as the complex/legacy nature of IT infrastructure and their boards' lack of awareness of risk reporting limitations. Anecdotally, the Principles may be less challenging for the D-SIBs to implement because their operations are restricted to their domestic market and/or their business models are less complex. Nevertheless, the D-SIBs should not underestimate the efforts needed to fully comply with the Principles.

There is a feedback loop between G-SIBs' and D-SIBs' implementation of the Principles, in instances where D-SIBs are subsidiaries of G-SIBs. A D-SIB's implementation of the Principles could be hampered if its G-SIB parent's implementation plan (eg IT system enhancements) is not well coordinated with that of the D-SIB. Similarly, poor implementation of the Principles by a D-SIB subsidiary will inevitably affect the G-SIB's ability to comply with the Principles as a banking group.

4. Key recommendations

Based on the quantitative assessment results and key observations in Section 2, the recommendations in the previous progress reports continue to be relevant as the challenges identified in previous assessments still persist. In addition, the RDN has identified three new recommendations to continue to promote effective and timely implementation of the Principles.

4.1. Banks should continue to implement the Principles in line with their roadmaps and consider how implementation would benefit other initiatives

4.1.1. Concrete actions should be taken in line with the bank's roadmaps

Banks should take concrete actions and continue to make progress in the implementation of the Principles according to the roadmaps as agreed with their supervisors. As the compliance deadline has already passed, further delays should be avoided.

The board and senior management should be strongly committed and ensure that the bank has:

- a well-established group risk data governance framework approved by the board;
- dedicated oversight from board and senior management specifically for the implementation of the Principles;
- strategic solutions for data architecture and IT infrastructure;

[10] It should be noted that this information is derived, in part, from D-SIBs' self-assessments of their implementation of the Principles, which could be overly optimistic.

- clear ownership of data for functional levels, including business and IT functions; and
- an internal validation unit to ensure proper implementation.

4.1.2. Consider how implementation of the Principles would benefit other initiatives

Some supervisors have noted that their banks have focused on the implementation of the Principles mainly as it pertains to their business operations. This is understandable, given the Principles' scope of application. But less attention has been paid to whether the upgraded RDARR practices would allow banks to comply effectively with other initiatives and requirements relating to data.[11]

Nevertheless, banks are encouraged to consider how the upgrades to their RDARR practices will let them comply more effectively with other initiatives and requirements relating to data (eg recovery and resolution plans). Improvements in a bank's ability to aggregate risk data could enhance its resolvability.[12] For recovery purposes, a robust data framework would help banks and supervisors anticipate problems ahead. When a bank comes under severe stress, it could also improve the prospects of finding alternative options for restoring financial strength and viability.

4.2. Supervisors should maintain supervisory intensity to ensure banks' implementation of the Principles and continue to promote home-host cooperation

4.2.1. Maintaining supervisory intensity

Supervisors are encouraged to maintain supervisory intensity to ensure banks' compliance with the Principles, and to:

- meet with the banks' board of directors and/or senior management in 2018, and regularly thereafter, to assess banks' implementation progress, based on the agreed roadmap.
- Consider combining off-site supervision of banks' implementation of the Principles with on-site inspections. Given the need to assess banks' data architecture and IT systems and their ability to aggregate risk data and generate risk reports, on-site supervision tends to better suited for this purpose. For example, on-site supervision would help establish the effectiveness of the bank's data quality framework and whether it has been properly implemented into its daily data quality management.
- Supervisors should continue to apply/escalate supervisory measures as required. This includes the more stringent measures within their supervisory toolkit such as capital add-ons and restrictions of the bank's business activities.

4.2.2. Continue to promote home-host cooperation

Supervisors are encouraged to share their supervisory methodologies regarding the implementation of the Principles on platforms such as the RDN, and through supervisory colleges and Crisis Management Groups. This will help to facilitate consistent application of supervisory expectations for global banking groups when implementing the Principles on a group-wide basis.

[11] Examples of such other initiatives and requirements include data reporting requirements arising from the Basel III and the Solvency II rules; recovery and resolution plans; and revisions to the supervisory reporting frameworks of financial reporting (FINREP) and common reporting (COREP) as well as to the international financial reporting standards (IFRS) and to the Foreign Account Tax Compliance Act (FATCA).

[12] For more information, see FSB, *Key Attributes of Effective Resolution Regimes for Financial Institutions*, October 2014.

4.3. Continuation of implementation monitoring efforts by the RDN

G-SIB supervisors will meet with banks' boards of directors and/or senior management in 2018 to obtain an update of the banks' progress in their implementation of the Principles, based on the roadmap agreed with their supervisors (see Section 4.2.1). The RDN plans to conduct the next implementation monitoring exercises in 2019.

Appendix 1: Summary of the Principles

The Principles cover four closely related sections:

- Overarching governance and infrastructure
- Risk data aggregation capabilities
- Risk reporting practices
- Supervisory review, tools and cooperation

I. Overarching governance and infrastructure

Principle 1

Governance – A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other principles and guidance established by the Basel Committee.[13]

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.

II. Risk data aggregation capabilities

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.

Principle 4

Completeness – 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, concentrations and emerging risks.

[13] For instance, the Basel Committee's, *Enhancements to the Basel II framework*, July 2009, and *Principles for enhancing corporate governance*, October 2010.

Principle 5

Timeliness – A bank should be able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, set based on the characteristics and overall risk profile of the bank.

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.

III. Risk reporting practices

Principle 7

Accuracy – Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.

Principle 8

Comprehensiveness – 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.

Principle 9

Clarity and usefulness – Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making. Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. Reports should include meaningful information tailored to the needs of the recipients.

Principle 10

Frequency – The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis.

Principle 11

Distribution – Risk management reports should be distributed to the relevant parties and while ensuring confidentiality is maintained.

IV. Supervisory review, tools and cooperation

Principle 12

Review – Supervisors should periodically review and evaluate a bank's compliance with the 11 Principles above.

Principle 13

Remedial actions and supervisory measures – Supervisors should have and use the appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies in its risk data aggregation capabilities and risk reporting practices. Supervisors should have the ability to use a range of tools, including Pillar 2.

Principle 14

Home/host cooperation – Supervisors should cooperate with relevant supervisors in other jurisdictions regarding the supervision and review of the Principles, and the implementation of any remedial action if necessary.

Appendix 2: Detailed assessment of compliance among G-SIBs by principle group

This Appendix sets out supervisors' assessments of banks' compliance levels by principle group, and gives examples of how banks have complied with the various principles or remedied the deficiencies observed. The examples set out in the 2016 assessment have been retained. Additional examples have been included arising from the 2017 assessment. The following examples are strictly for illustration purposes and not meant to be interpreted as guidance on implementation.

1. Overarching governance and infrastructure (Principles 1–2)

1.1. Governance

Supervisors have largely utilised existing supervisory tools or examination methods to assess risk data governance. Some supervisors have developed examination templates or procedures for reviewing a firm's governance of the Principles in the interests of consistency. Several supervisors meet regularly with bank management and the board, and review the relevant board and senior management documentation, such as organisational charts, meeting minutes from appropriate committees (eg audit committee, enterprise risk committee) and the related governance and control framework documentation. In reviewing the effectiveness of risk data governance, supervisors have assessed the level of a bank's oversight and funding for projects aimed at implementing the Principles, and they have also determined whether senior management and/or the relevant committee are appropriately empowered to execute these project(s).

Examples of effective governance demonstrated by banks that were rated as fully or largely compliant are:

- Integration of risk data governance into the overall risk management framework.
- Establishment of definitions of bank-wide data requirements.
- Policies in place setting out a clear delineation of roles, incentive schemes and responsibilities for risk data management (including dedicated staff responsible for defining risk data expectations), data quality and creation and distribution of risk reports. For example, business departments own the data and are responsible for risk data monitoring, analysis, and management throughout the data life cycle; and risk management departments take a leading role in compiling the comprehensive risk reporting.
- Effective and audience-appropriate communication at regular intervals. For example, senior management communicates risk data implementation initiatives to the board of directors or the appropriate board committee, and there are well established communication initiatives explaining risk data efforts throughout the bank. There are also open lines of communication among business lines as exhibited by regular interdepartmental meetings on data governance or the development of new training materials for bank staff.
- Independent functions, internal or external, have reviewed risk data implementation efforts and have shared any material weaknesses or deficiencies with the appropriate level of bank management. There is regular independent validation of risk data aggregation and reporting processes.
- Application of Principles to internal reporting, regulatory reporting and financial reporting.

Examples of ineffective governance and key compliance gaps of banks are:

- Lack of structured policies and frameworks to consistently assess and report risk data aggregation and risk reporting implementation activities to the board and senior management. For instance, RDARR policies are not approved or not fully developed across the enterprise or global organisation.
- Plugging gaps in an ad hoc manner, rather than focusing on holistically improving governance capabilities that are consistent with the Principles.
- Lack of clearly assigned accountability/insufficient authority assigned to staff for the development of a well defined enterprise data programme.
- Inadequate data governance approaches. For instance, reporting governance is not fully consistent among legal entities; data ownership is insufficiently defined or risk reporting owners cannot readily demonstrate that all required data and reporting controls are implemented.
- Ineffective or weak project management practices. For example:
  - Large-scale IT projects or strategy designed to implement the Principles are incomplete, or in some cases lack a detailed project schedule for the finalisation of needed improvements.
  - Lack of transparent status, progress, and cost reporting to inform key stakeholders of implementation progress.
  - Inappropriate identification of project scope or an insufficiently comprehensive list of risk reports to consider.
  - Inadequate technical expertise on project teams, making it difficult to inform governance committees thereby creating delivery or decision bottlenecks.
- Lack of communication on the limitations of RDARR practices to key stakeholders.
- Training plans need to be improved to enhance awareness of staff in charge of data quality.
- Merger and acquisition activities, as well as other initiatives such as divestitures, new product development and IT developments, did not always take into account the potential impact of critical data elements and how those updates should be applied to the overall RDARR framework.
- Insufficient independent validation.

1.2. Data architecture and IT infrastructure

Supervisors continue to utilise qualitative and quantitative methodologies to review banks' data architecture and IT infrastructure with regard to risk data implementation. Examples of methodologies adopted include reviewing specific metrics in data architecture for RDARR purposes (eg proportion of key risk measures available on reporting dashboard); leveraging on technical IT staff to gain insight into banks' data architecture and IT infrastructure (eg participation of IT examination staff in risk data-specific assessments); and assessing a bank's capacity to produce timely data in times of stress. Some supervisors also reviewed the work completed by the firm's internal audit function, and track progress on the remediation of issues on an on-going basis until they are resolved. This exercise also allowed supervisors to validate the adequacy of the internal audit's opinion and findings.

Examples of effective data architecture and IT infrastructure demonstrated by banks that were rated as fully or largely compliant are:

- Allocation of appropriate resources to effectively integrate previously isolated databases from disparate legal entities, subsidiaries and branches.
- Identification of redundant or inefficient technologies and processes, streamlining IT platforms and systems.
- Consolidation of data categorisation approaches and structures as well as integrated data taxonomies. A data dictionary and a single data repository or data warehouse for each risk type are identified and constructed. Effective measures are put in place to manage customer information and utilise industry taxonomy (eg the Legal Entity Identifier (LEI)).[14]
- Projects on data quality assessments and data remediation have been conducted across all business units, sometimes with the use of scorecards.
- Establishment of effective business continuity plans of IT systems in case of crisis, with the backup data systems tested periodically. For example, data warehouse and risk analysis systems are all included in the crisis backup system. Detailed plans and action measures are in place for data warehouse continuity, as well as crisis backup capabilities.

Examples of ineffective data architecture and IT infrastructure and key compliance gaps of banks are:

- Failure to complete IT infrastructure projects, resulting in the continued use of disparate or legacy IT systems that generate poor data quality and aggregation possibilities.
- Dependence on manually intensive processes or end user computing for most routine risk reports and ad hoc reports without sufficient controls or adequate testing of manual controls.
- Lack of appropriate processes and controls to ensure that the risk reference data is updated following changes in business activities and a lack of a formalised escalation process to communicate poor data quality to senior management.
- Inability to integrate data taxonomies and architecture from certain foreign subsidiaries into the banking group. This can arise from non-existent, inconsistent, unintegrated, and/or imprecise data dictionaries, data models, data taxonomies, and/or definitions. For example, inconsistent customer codes are used within the bank or there is a lack of data dictionaries for certain risk types, such as operational risk.
- Certain activities from the first and second lines of defense are not fully implemented, which negatively impact banks attempting to deploy an integrated IT approach. As a result, there is a lack of an end-to-end ownership model for critical data throughout the data lifecycle to enable ongoing data oversight and remediation.
- Inability to produce data and reports, even for major risk categories, in both normal times and stressed scenarios.

2. Risk data aggregation capabilities (Principles 3–6)

Supervisors reviewed different types of risk report to assess banks' data accuracy, timeliness and completeness as well as the adaptability of their risk data aggregation capability in meeting reporting requests by different parties (eg internal needs, supervisory queries) under different scenarios (eg ad hoc and stress situations). Data obtained from other sources (eg regulatory reports and stress-testing exercise) were also assessed.

[14] LEI availability could enhance banks' management of information across legal entities, facilitate a comprehensive assessment of risk exposures at the global consolidated level and improve the speed at which information is available internally and to supervisors, especially after a merger or acquisition.

Some supervisors have also explored the use of fire drills to perform ad hoc assessments of banks' abilities to promptly respond to ad hoc risk data requests, and relied on banks' internal audit functions to validate, or certify, the completeness and accuracy of data produced in response to such requests. These tests highlight the importance of having a clear understanding of the data content required in both regular and stress situations.

Examples of effective risk data aggregation demonstrated by banks that were rated as fully or largely compliant are:

- Implementation of IT capabilities to aggregate foreign subsidiary data automatically. For instance, using a metadata model developed at group level, one bank was able to integrate and centralise basic data for all risk types.
- Integrated data taxonomies established across the banking group.
- Proper data quality controls. For example, there is appropriate data element certification, data quality documentation, data quality assurance mechanisms, assessment of data quality per risk type, documented and effective controls for manual processes. In this respect, one bank introduced units responsible for data quality for all entities globally.
- Proper data reconciliation framework across the bank. For example, there is consistent monitoring and formalisation of reconciliation processes (primarily by providing a rationale for differing reconciliation methodologies and results); and reconciliation requirements are established. In some instances, improvements in the coordination and reconciliation of risk, finance and regulatory data were noted.
- Timely adjustments of risk data aggregation methods and procedures in response to business development, risks and regulatory changes.

Examples of ineffective risk data aggregation and key compliance gaps are:

- Lack of progress, due to dependence on strategic IT systems yet to be rolled out.
- Deficiencies in data quality controls. For example, inability to map and integrate data quality standards; data quality rules such as minimum standards for data quality reporting thresholds not properly established; absence of a designated authority to oversee the effectiveness of data quality rules and reporting framework developed by local risk functions; lack of an effective escalation model for data quality issues; and weaknesses in data quality checks such as non-blocking validation controls.
- Notable presence of/overreliance on manual risk data aggregation processes without proper documentation and manual data amendment policy.
- Lack of reconciliation for certain key reports (eg reconciliation between risk and finance data) and no variance analysis to determine if there are any changes in reports over time.
- Inability to promptly source risk data from foreign subsidiaries and to automatically aggregate risk data from overseas subsidiaries and institutions due to system constraints.
- Lack of standardisation of reference data for risk aggregation and reporting by risk and finance functions.

3. Risk reporting practices (Principles 7–11)

In general, supervisors reviewed risk reporting practices as part of the normal supervisory process. Supervisors assessed risk reporting practices by reviewing reports catering to various levels including the board, senior management and staff to ensure the content, granularity and frequency were appropriate.

In some cases, supervisors carried out fire-drill exercises to assess whether banks could accurately and comprehensively report a number of selected data points within a tight deadline.

Examples of effective risk reporting practices demonstrated by banks that were rated as fully or largely compliant are:

- Production of accurate and timely reports in both business-as-usual and stressed situations. The bank's risk management reports are promptly and properly distributed to the relevant internal parties (including the board of directors and senior management) and external regulatory authorities.
- The business-as-usual risk reports have certain proactive or dynamic characteristics that support the analysis of various risk types and drill-down of risk data and can be promptly represented via a user-friendly panel and interface.
- Risk reports (i) focus on the analysis of change in risk trends and potential risk issues; (ii) feature early testing using scenario analysis and stress testing; and (iii) contain risk management measures. When appropriate, banks have also standardised "top of the house" reporting, resulting in consistent identification and communication of risk trends.
- Risk management departments maintain procedures or guidelines for ad hoc reports that let them produce consistently accurate and tailored reports for the appropriate audience.
- Critical reports are subject to validation.
- Most of the reports are generated automatically with clear and reliable source data. Manual reports are either in the process of being automated, or contain appropriate controls to ensure report accuracy.
- Risk reports cover all vital risk types (eg credit, market, operational, liquidity, reputational, IT and country risks) as well as material concentrations in key industries, products or geographies.
- Risk reports are created at the appropriate frequency and are tailored to the board and senior management. In particular, the focus of the reports is clear, showing where specific items have been highlighted for management's attention and action. The reports are also sufficiently detailed in terms of content, enabling the board and/or senior management to make informed decisions.
- The board and senior management have taken steps to identify the scope of data necessary to deal with a crisis and prepare report templates for the data in advance.
- A unified distribution channel for reporting serves as a single point of entry for all relevant risk reporting with different levels of access defined by profiles, which are managed centrally. The report distribution channel is strictly controlled. Through encryption of files and authority control by information system, the confidentiality of risk reporting is ensured appropriately.

Examples of ineffective risk reporting and key compliance gaps of banks are:

- Reports are static in nature and not complemented by more dynamic dashboard-type reporting.
- Overreliance on manual processes to produce reports. These manual processes also hindered banks from producing reports quickly, in particular ad hoc reports for special requests or crisis situations.
- Inability to produce risk reports in a timely manner under stress scenarios.
- Risk reports not being sufficiently comprehensive. Examples include:
    - Insufficiently granular data in certain businesses or areas. For example, risk reports that do not show the breakdown of information into different risk categories and subcategories (eg general credit risk and counterparty credit risk).

- Lack of information on forward-looking forecasts and stress tests, hindering users who need to monitor emerging trends.
- Incomplete risk reports because legal constraints prevent banks from gathering data from foreign subsidiaries.
- Different regions and countries sometimes have different risk packs and different risk measures with core metrics that are not fully aligned.

- Inaccuracies in risk reports. For example, some data are outdated due to complex processes to aggregate risk data and the extended time taken to approve the reports.
- Risk reports not being validated because of insufficient controls and inadequate validation rules or procedures. Processes to report and remediate data quality errors in risk reports are not embedded into the daily business processes.

4. Supervisory review, tools and cooperation (Principles 12–14)

4.1 Supervisory review of banks' compliance

The role of supervisors in the promotion of BCBS 239 implementation has been continuously enhanced.

Principle 12 states that supervisors should periodically review and evaluate a bank's compliance with the Principles. Almost all supervisors used the banks' self-assessments to feed into their own supervisory activities and assessments. Some supervisors performed risk-specific supervisory activities or carried out thematic reviews of multiple banks. In some cases, supervisors used banks' internal audit functions or external auditors to evidence levels of compliance in order to complement their own assessment.

4.2 Supervisory follow-up measures to address non-compliance

Principle 13 states that supervisors should have and use the appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies in its RDARR practices.

In terms of the supervisory process, upon completing any examination activities, supervisors will issue follow-up letters or examination reports to banks setting out their deficiencies. In response to such letters or examination reports, banks should highlight in their roadmaps how such implementation gaps (if any) would be closed. In general, supervisors can use independent reviews, such as internal or external audits, to assess implementation efforts. Some supervisors raised concerns with the banks on the slow implementation progress past the deadline of 2016 and informed them that the overall supervisory review will take into account their compliance with the Principles, meaning that insufficient progress could result in a higher Pillar II capital add-on.

In general, however, the supervision of banks' implementation of the Principles proceeds in line with the supervision of other activities. For example, supervisors have increased the intensity of their work vis-à-vis banks with deficiencies in implementing the Principles. Supervisors have also required banks to deliver implementation roadmaps and to take remedial action within a specific time frame. Also at the disposal of some supervisors are potential restrictions on banks' business activities or capital distributions.

Examples of actions that banks were requested to take or unilaterally took following risk data examinations include:

Governance

- Establishing a board-level committee responsible for data governance, integrity and quality.

- Requiring senior management to keep the board of directors informed of enterprise risk data governance framework developments (formalising an escalation process for informing board and senior management).
- Updating appropriate policies to clearly describe processes for compiling accurate, comprehensive and transparent risk reports.
- Hiring new leadership to institute an improved enterprise risk data governance framework
- Improving reporting of risk data and risk reporting project initiatives, so that they are reviewed with other high priority strategic initiatives.
- Expanding the scope of risk data project plans, such as migrating from tactical solutions to longer term strategic solutions.
- Increasing the scope and quality of validation by internal audit.
- Developing plans to reduce the reliance on manual processes and enhance end user controls as well as enhancing testing processes in areas where manual controls cannot be fully eliminated.
- Creating training plans to inform bank staff and senior management of data quality initiatives and practices.

Data architecture and IT infrastructure

- Reaffirming the banks' commitment to fund longer-term projects aimed at supporting critical IT infrastructure that will assist in the banks aggregating data and complying with the Principles.
- Updating data standards and ensuring they are applied to the business lines and overseas subsidiaries.
- Improving the level of automation for risk data collection in IT systems. This includes developing plans to reduce the reliance on manual processes and enhance end user controls in areas where manual controls cannot be fully eliminated.
- For banks looking to acquire other institutions, to consider the entity's risk data aggregation and risk-reporting capabilities and issues, and understanding the impact of such an acquisition on risk data and relevant IT systems.

Data aggregation

- Working with the host supervisors of the bank's subsidiaries to receive permission to gather appropriate risk data.
- Increasing staffing for managing and implementing risk data aggregation processes and procedures.
- Increasing the number of ad hoc exercises and stress scenarios involving the production of aggregate risk reports and developing a framework for producing ad hoc reports.
- Formulating programmes for enhancing risk data checks and analyses of data quality problems.

Risk reporting

- Monitoring the appropriateness of previously identified key risk reports, and adding any new risk reports based on new business activities or risks. This could potentially include establishing a plan to apply the Principles to regulatory reporting.
- Developing methodologies to assess the comprehensiveness of risk reports.

- Periodically examining the capability to produce risk reports in crisis or stress situations.
- Stress-testing initiatives to evaluate the overall effect of credit, market and operational risks in a consolidated stress scenario.

While not targeted specifically at the G-SIBs, some initiatives may affect their risk aggregation capabilities and could be supported by authorities to foster compliance with the Principles. For instance, some supervisors promote the use of LEI and/or support the work on integrated data taxonomies.

4.3. Home-host cooperation

Principle 14 states that supervisors should cooperate with relevant supervisors in other jurisdictions regarding the supervision and review of the Principles and the implementation of any remedial action if necessary. In this regard, supervisors are generally satisfied with the existing communication channels through supervisory colleges, crisis management groups and bilateral contacts. Given the feedback loop between G-SIBs' and D-SIBs' implementation of the Principles, there should be open communication and coordination between G-SIB and D-SIB supervisors via the relevant communication channels.

Appendix 3: Banks identified as G-SIBs during 2011–17[15]

Jurisdiction	Banks
Canada	Royal Bank of Canada
China	Agricultural Bank of China Bank of China China Construction Bank Industrial and Commercial Bank of China Limited
France	BNP Paribas Groupe BPCE Groupe Crédit Agricole Société Générale
Germany	Commerzbank Deutsche Bank
Italy	Unicredit Group
Japan	Mitsubishi UFJ FG Mizuho FG Sumitomo Mitsui FG
Netherlands	ING Bank
Spain	BBVA Santander
Sweden	Nordea
Switzerland	Credit Suisse UBS
United Kingdom	Barclays HSBC Lloyds Banking Group Royal Bank of Scotland Standard Chartered
United States	Bank of America Bank of New York Mellon Citigroup Goldman Sachs JPMorgan Chase Morgan Stanley State Street Wells Fargo

[15] Dexia is undergoing an orderly resolution process.

Appendix 4: Members of the Risk Data Network

Chair: Sunny Yung (Hong Kong Monetary Authority)

Canada	Bob Hassan	Office of the Superintendent of Financial Institutions
China	Song Lijian	China Banking Regulatory Commission
France	Jean Patrick Yanitch	French Prudential Supervision and Resolution Authority
Germany	Stefan Iwankowski	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
	Marina Zaruk	Deutsche Bundesbank
Hong Kong SAR	Sophia Chan	Hong Kong Monetary Authority
Italy	Vicenzo Maria Re	Bank of Italy
Japan	Shigeo Kawauchi	Bank of Japan
	Shigeru Osuga	Financial Services Agency
Netherlands	Bart Luppes	Netherlands Bank
Russia	Marina Eminova	Central Bank of the Russian Federation
Saudi Arabia	Waleed Almaqawshi	Saudi Arabian Monetary Authority
South Africa	Jacques Henning	Prudential Authority South African Reserve Bank
Spain	Pilar Puig	Bank of Spain
Sweden	Maximilian Gortz	Finansinspektionen
Switzerland	Alexandre Kurth	Swiss Financial Market Supervisory Authority (FINMA)
United Kingdom	Carl Taylor	Prudential Regulation Authority
United States	Alex Kobulsky	Board of Governors of the Federal Reserve System
	Irina Leonova	Federal Deposit Insurance Corporation
	Kianne Gumbs	Federal Reserve Bank of New York
	Tom Crock	Office of the Comptroller of the Currency
EU	Nicola Papa	European Central Bank
Financial Stability Board	Gianmatteo Piazza	Financial Stability Board
	Grace Sone	
BCBS Secretariat	Ethan Goh	Secretariat