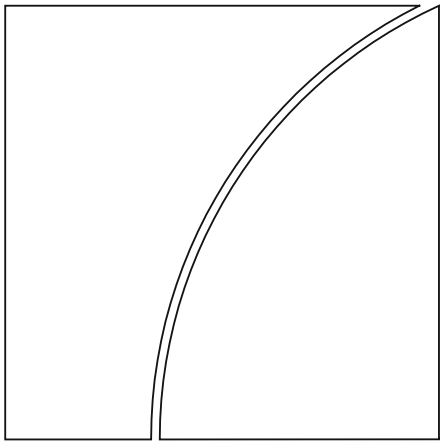
Basel Committee
on Banking Supervision



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

March 2017

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*

In January 2013, the Basel Committee published the *Principles for effective risk data aggregation and risk reporting* ("the Principles").[1] The Principles aim to strengthen banks' risk data aggregation capabilities and internal risk reporting practices, and became effective in January 2016. Since the publication of this framework, the Basel Committee has been monitoring banks' implementation.

The latest assessments by supervisors show that banks' level of compliance is unsatisfactory and the overall implementation progress remains a source of concern to supervisors. Based on supervisors' assessments, only one bank fully complied with the Principles, even though the implementation deadline for global systemically important banks (G-SIBs) identified in 2011 and 2012 had lapsed in January 2016. In view of the unsatisfactory assessment results, banks are urged to step up efforts to comply with the Principles. Supervisors are expected to monitor progress and call on banks to address observed weaknesses.

The objective of this report is to analyse banks' progress on compliance with the Principles, identify key deficiencies and propose key recommendations to further facilitate implementation. Section 1 summarises the objectives of the Principles and the work conducted to date. Section 2 provides an overview of banks' extent of compliance with the Principles, including the key observations of supervisors regarding the main deficiencies from banks' current implementation strategies. Section 3 discusses domestic systemically important banks' (D-SIBs') implementation of the Principles. Section 4 proposes recommendations for banks and supervisors in the near to medium term.

1. Objectives of the Principles and work to date

1.1 Objectives of the Principles

The Principles were developed in response to the global financial crisis of 2007–09 and are intended to:

- enhance the infrastructure for reporting key information, particularly for board and senior management;
- improve the decision-making process throughout the bank by enhancing the management of information across legal entities and at the global consolidated level;
- reduce the probability and severity of losses resulting from risk management weaknesses;
- improve the speed at which information is available and hence decisions can be made; and
- improve the bank's quality of strategic planning and the ability to manage the risk of new products and services.

Effective implementation of the Principles underpins sound risk management practices and decision-making processes at banks, in turn improving the resilience of the overall financial system. Improving banks' ability to aggregate risk data will also improve their resolvability.

In order to achieve these benefits, the Principles provide guidance on the infrastructure and capacities that banks should have in place to improve risk management. The 11 Principles applicable to

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

banks can be classified into three main areas: (i) governance and infrastructure; (ii) data aggregation; and (iii) risk reporting (see Appendix 1).

There are also three Principles targeted at supervisors regarding the supervision of banks' compliance with the Principles. The main objectives of these three Principles are to ensure that supervisors periodically review and evaluate banks' compliance, have the appropriate toolkit to ensure that banks follow the Principles, and promote home-host cooperation.

1.2 Committee work to date

The implementation deadline for the Principles for banks identified as G-SIBs in November 2011 or November 2012[2] was January 2016.

The Committee, via the Risk Data Network under the Committee's Supervision and Implementation Group,[3] had been monitoring implementation of the Principles since its publication in January 2013. Over 2013–15, the Committee published three reports. In 2013 and 2014, the reports were based on banks' self-assessments of their progress towards compliance with the Principles. The Committee also conducted outreach with private sector stakeholders to better understand implementation challenges. In 2015, the Committee's monitoring efforts focused on drawing out key lessons learned from the previous self-assessments and supervisory work to form a more complete picture of how supervisors should incorporate the review of the Principles into their supervisory programmes.

In 2016, the Committee continued to carry on the monitoring work for risk data, but with a stronger focus on supervisory evaluations and adopting an evidence-based approach to monitoring. In July 2016, supervisors were asked to complete a questionnaire to assess their banks' progress on compliance with the Principles. The supervisory assessments form the basis for this report.

2. Assessment results and key observations

The 2016 supervisors' assessment questionnaire was completed by all seven supervisors / supervisory regimes that had G-SIBs under their supervision. The questionnaire responses included 30 banks which were designated as G-SIBs in 2011 or 2012 and were subject to the January 2016 implementation deadline.

2.1 Overview of assessment results

In the 2016 questionnaire, supervisors were asked to rate their banks' current levels of compliance with each of the risk data aggregation and risk reporting (RDARR) Principles on a 1 to 4 scale. The four ratings were defined as follows:

- Rating of 4 – *The Principle is fully complied with*: The objective of the Principle is fully achieved with the existing architecture and processes.

[2] G-SIBs designated in subsequent annual updates will need to comply with the Principles within three years of their designation. The framework suggests a similar time frame for designated D-SIBs.

[3] The Risk Data Network's objective is to support the Committee's Supervision and Implementation Group to foster sound and consistent implementation of the Principles. A list of the members of the Risk Data Network is in Appendix 4.

- 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.
- Rating of 1 – *The Principle has not been implemented*.

2.1.1 Levels of compliance

Banks have not complied fully with the Principles, even though the implementation deadline of January 2016 has now lapsed. Graph 1 shows that for no Principle was full compliance reached by all assessed banks. Although all Principles except Principle 2 (data architecture and IT infrastructure) were largely or fully complied with by over half of the assessed banks, only one bank fully complied with all the Principles. Principle 2 had the largest number of banks (15, or 50%, of total number of banks) which were assessed to be materially non-compliant or have not implemented the Principle. This is of particular concern to supervisors because Principle 2 is one of the two preconditions (together with Principle 1 on governance) to ensure compliance with the other Principles.

Graph 1 – Levels of compliance by Principle

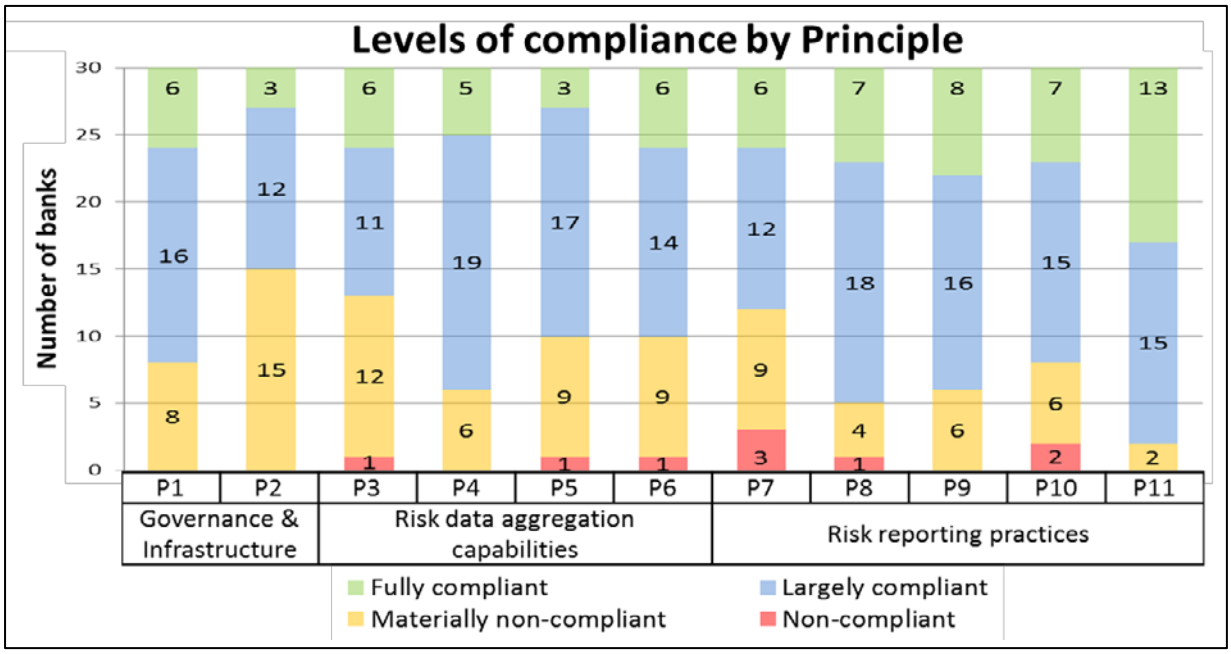


Table 1 – Average compliance ratings of banks

Assessment	Governance & infrastructure		Risk data aggregation capabilities				Risk reporting practices				
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
2016	2.93	2.60	2.73	2.97	2.73	2.83	2.70	3.03	3.07	2.90	3.37

In the 2016 assessment, the average compliance ratings by Principle of the assessed banks ranged from 2.60 to 3.37. The average ratings of most of the Principles were still below the largely compliant level (ie below a rating of 3). Principle 2 (data architecture and IT infrastructure) had the lowest average compliance rating (2.60). Only three Principles attained an average rating of the largely

compliant level (ie a rating of 3 or above), namely Principle 8 (comprehensiveness), Principle 9 (clarity and usefulness) and Principle 11 (distribution) of risk reporting practices.

The detailed assessment of compliance with the Principles, by Principle group, can be found in Appendix 2.

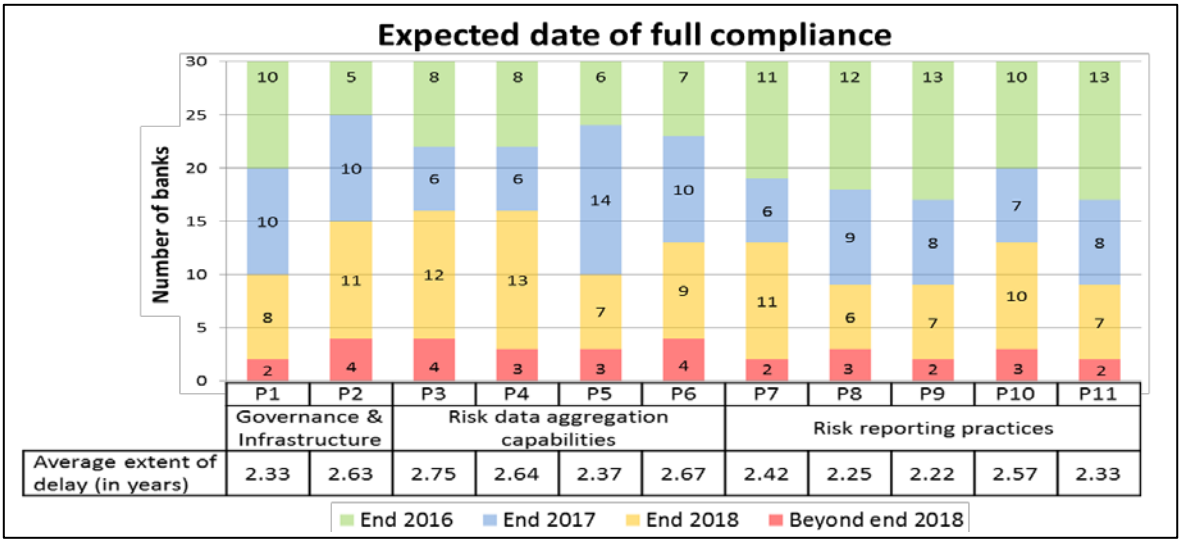
2.1.2 Expected date of compliance

It is worth highlighting that only one bank had achieved full compliance with all Principles by the deadline, with another bank expected to achieve full compliance at the time of publication of this report. Twenty-four banks are expected to achieve full compliance at or before end-2018. Four banks are expected by supervisors to fully comply with all the Principles beyond 2018.

The 2016 assessments reflected that, in general, banks would take about five to six years to achieve full compliance, assuming that they started implementation work when the Principles were published in January 2013.

Graph 2 shows that, for banks which failed to meet the January 2016 implementation deadline, the average delay in implementation of individual Principles ranges from 2.22 to 2.75 years. Although many banks are expected to achieve full compliance in two to three years, the execution risk of not meeting the expected date of full compliance remains a concern. It is therefore critical for banks and supervisors to place a high priority on full implementation of the Principles in a timely manner.

Graph 2 – Expected date of full compliance



Note:

1. "Average extent of delay" reflects the average number of years of delay of banks that missed the January 2016 deadline for individual Principles. "Average extent of delay" is the difference between the expected date of full compliance and the January 2016 deadline. For example, an expected date of full compliance by end-2016 represents one year of delay, and so forth.
2. The "End-2016" group includes banks that had achieved full compliance by the January 2016 deadline and banks that were expected to achieve full compliance by end-2016.

2.2 Key observations

2.2.1 Some improvements by banks in 2016 but substantial work towards full implementation needed

Overall, banks have made some progress in implementing the Principles (see Section 2.1.1). Over the years, supervisors have communicated to banks areas of particular concern with regard to implementing the Principles. Most G-SIB boards are increasingly recognising the importance of the Principles. Senior management are appropriately involved in the implementation process. Banks have also improved their risk data governance structures (eg established data governance committees and senior-level positions) as well as their abilities in aggregating and reporting data in some risk areas. Despite this progress, substantial work has to be done by banks to implement the Principles in full.

2.2.2 Challenges faced by banks

Banks continue to face challenges when implementing the Principles, in terms of (i) technical issues and (ii) defining and assessing materiality.

Technical issues

Major technical issues 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, although some manual processes are unavoidable.
- Incomplete integration and implementation of bank-wide data architecture and frameworks (eg data taxonomies, data dictionaries, risk data policies).
- Weaknesses in data quality controls (eg reconciliation, validation checks, data quality standards).

Defining and assessing materiality

Under the Principles, the concept of materiality means that data and reports can exclude information only if it does not affect the decision-making processes in banks. In applying the materiality concept, banks need to take into account considerations such as the size of the exposures concerned, types of risk involved, and dynamic nature of the banking business. Defining materiality is one of the challenges of effectively implementing the Principles as highlighted in the progress report of December 2015, as the concept of materiality is idiosyncratic and varies depending on banks' business models and risk exposures.

In the 2016 supervisors' assessments, supervisors observe that banks continue to find the determination of materiality thresholds which are acceptable to their supervisors to be challenging. Examples of approaches adopted in practice:

- One supervisor required banks' internal audits to review the adequacy of the definition of materiality, ie what risk types, functions, business units and legal entities are considered material for decision-making at senior management level, and whether all material risk types, functions, business units and legal entities have been covered by banks' RDARR programmes.
- One supervisor has applied proportionality in assessing banks' compliance with the Principles (ie giving different weighting to individual risk types for banks with different business models). For instance, greater weighting is given to assessments of market risk for an investment bank than a retail or commercial bank.

As highlighted in the 2015 progress report, banks' board and senior management have the primary responsibility for defining materiality in a way that best suits their business models and risk profiles. Banks should clearly articulate their expectations on RDARR, including the definition of materiality, and should explain their interpretation of the Principles and chosen definition of materiality to supervisors.

2.2.3 Compliance with the Principles needs to be dynamic and forward-looking

Some banks view implementing the Principles as a one-time compliance exercise rather than a dynamic and ongoing process. Supervisors noticed that some banks did not have due consideration of RDARR requirements when pursuing new business initiatives. Any changes in banks' business models and risk profiles as well as new strategic initiatives (eg mergers and acquisitions) are likely to bring about new implementation challenges. It is also observed that some banks faced challenges in detecting and monitoring emerging trends through forward-looking forecasts and stress tests.

In this regard, banks need to periodically assess and make needed improvements to IT systems, policies and processes to effectively implement the Principles.

2.2.4 Supervisors have structured supervisory approaches and toolkits to assess banks' compliance and deal with banks' deficiencies

Supervisors adopted structured approaches in 2016 to assess banks' compliance with the Principles, though in different forms such as regular supervisory reviews, thematic reviews, auditors' reviews and "fire drill".

In addition, supervisors' responses indicate that there are numerous supervisory follow-up measures for dealing with banks with noted RDARR deficiencies. Supervisory measures that are available include requesting banks to take remedial actions within a specific time frame, asking banks to conduct independent reviews, increasing supervisory intensity, imposing capital add-ons, and restricting business activities.

3. Implementation by D-SIBs

National supervisors are strongly encouraged by the Basel Committee to apply the Principles to banks identified as D-SIBs, three years after their designation as D-SIBs.[4]

National supervisors, when applying the Principles to their D-SIBs, are encouraged to start the implementation process early, given the observation from the 2016 assessments that the G-SIBs would take about five to six years in general to achieve full compliance with the Principles.

[4] Paragraph 15 of the Principles states that "it is strongly suggested that national supervisors also apply these Principles to banks identified as D-SIBs by their national supervisors three years after their designation as D-SIBs".

4. Key recommendations

Based on the supervisors' assessment results and key observations above, the recommendations to banks in the 2015 progress report continue to be relevant, as some of the challenges identified in previous assessments still persist.[5]

In addition, the Committee proposes three new recommendations to continue to promote effective and timely implementation of the Principles. These recommendations suggest that banks and supervisors have key roles to play in further strengthening banks' risk data aggregation and risk reporting.

4.1 Banks should develop clear roadmaps to achieve full compliance with the Principles and to comply with the Principles on an ongoing basis

4.1.1 Development of clear roadmaps to achieve full compliance with the Principles

Almost all the assessed banks failed to meet the implementation deadline of January 2016. Banks are thus urged to enhance efforts to work towards full compliance and deliver against their own commitments.

Banks should provide clear roadmaps detailing how they intend to move towards full compliance with the Principles to their national supervisors by June 2017. A roadmap should minimally include:

- a timeline 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 which could be provided to demonstrate that implementation progress is being made.

4.1.2 Compliance with the Principles should be on an ongoing basis

It is crucial that compliance with the Principles takes place on an ongoing basis. In this regard, banks should thoroughly consider the possible implications for implementation of the Principles before making strategic planning decisions, such as mergers, acquisitions and business expansions. The Principles should also be embedded into banks' ongoing risk management frameworks to ensure that RDARR are integrated into every part of their risk management activities. Senior management should promote an organisation-wide culture whereby RDARR requirements are taken into consideration whenever there are changes in business models and risk profiles.

[5] The following recommendations to banks as set out in the 2015 progress report remain relevant:

- Banks and supervisors should continue to promote understanding of the Principles.
- Banks should clearly articulate risk data aggregation and risk reporting expectations, in line with their risk appetite in both normal and stress periods.
- Banks should have effective governance arrangements in place for manual processes to ensure that they are appropriately controlled and comply with the Principles.
- Banks should critically examine their data architecture and data adaptability capabilities.
- In cases of non-compliance at the implementation deadline, banks should provide a remedial plan that is agreeable to supervisors.

4.2 Supervisors should communicate assessment results with individual banks, incentivise banks to achieve full compliance with the Principles and continue to refine assessment techniques

4.2.1 Communication of individual banks' assessment results

Supervisors should communicate details of their assessment results to the banks' board of directors and senior management by June 2017. The communication should highlight any key areas of concerns so that banks can focus on those areas and devote greater efforts and resources to addressing them, instead of focusing on the relative compliance achieved. There should be ongoing communication between the supervisors and the bank's board of directors on the bank's implementation of the Principles, and, on a more frequent basis, with the bank's senior management.

In line with the recommendation in Section 4.1.1, supervisors should ask banks for their detailed roadmap and timelines to full compliance and details about their frameworks of top-level oversight of implementation progress.

4.2.2 Ways to incentivise banks to achieve full compliance

As noted in Section 2.1.2, banks in general would take about two to three more years to fully comply with the Principles. Supervisors should closely follow up on banks' RDARR weaknesses with continued and intensified efforts to ensure that banks would adhere to their committed timelines. In monitoring banks' remediation progress, supervisors should evaluate the effectiveness of the follow-up measures taken. Whenever necessary, supervisory actions should be taken to encourage banks to take the required actions to implement the Principles. Banks should be explicitly informed of any supervisory consequence if they fail to meet their implementation deadlines and are encouraged to conduct root cause analyses regarding further delay in implementation.

4.2.3 Refinement of assessment approaches and techniques

Supervisors should continue to refine their assessment approaches by applying their assessments of banks' compliance with the Principles across a comprehensive range of supervisory activities. Apart from conducting dedicated reviews, supervisors should also assess compliance through other regulatory and supervisory exercises. For instance, supervisors should consider the quality of data submitted for stress tests and regulatory reporting when assessing banks' RDARR effectiveness. In assessing compliance, supervisors should evaluate how banks articulate their definition of materially complying with or effectively implementing the Principles.

4.3 Continuation of implementation monitoring efforts by the Committee

Given the unsatisfactory results where only one bank had attained full compliance with the Principles by the January 2016 deadline and with another bank expected to achieve full compliance at the time of publication of this report, the Committee will continue to monitor the implementation of the Principles by banks and supervisors.

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.[6]

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.

[6] For instance, the Basel Committee's Principles for Enhancing Corporate Governance (October 2010) and enhancements to the Basel II framework (July 2009).

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 highlights supervisors' assessments of banks' compliance levels by Principle group and provides examples of how banks have complied with the various Principles and the deficiencies observed. The examples are strictly for illustration purposes and not meant to be interpreted as guidance on implementation.

1 Overarching governance and infrastructure (Principles 1 and 2)

1.1 Governance

Several supervisors noted the importance of meeting with bank management and reviewing 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 assessed the level of a bank's oversight and funding for projects aimed at implementing the Principles; as well as determining whether senior management and/or the relevant committee are appropriately empowered to execute the project(s) advancing implementation.

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

- Integration of risk data governance into the overall risk management framework.
- Establishment of definitions of bank-wide data requirements, and applicable policies clearly delineating the groups or departments responsible for ensuring data quality and for creating and distributing risk reports.
- Clear roles, incentive schemes and responsibilities for risk data management, including dedicated staff responsible for defining risk data expectations. For instance, business departments own the data and are responsible for risk data monitoring, analysis and management; and risk management departments take a leading role in compiling the comprehensive risk reporting.
- Effective and audience-appropriate communication. For instance, senior management communicate risk data implementation initiatives to the board of directors or appropriate board committee; and there are well established communication initiatives explaining risk data efforts throughout the bank.
- 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 RDARR Principles to regulatory and financial reporting.

Examples of ineffective governance and key compliance gaps of banks:

- Lack of structured policies and frameworks to consistently assess and report RDARR implementation activities to the board and senior management.

- RDARR policies are not approved or not fully developed across the enterprise or global organisation.
- Insufficient data governance approaches. For instance, 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 with regard to 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.
- Lack of communication on limitations of risk data aggregation and reporting practices to key stakeholders.
- Merger and acquisition activities did not always consider RDARR requirements.
- Insufficient independent validation.

1.2 Data architecture and IT infrastructure

Supervisors utilised qualitative and quantitative methodologies to review banks' data architecture and IT infrastructure with regard to risk data implementation. Examples of methodologies adopted are: 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 banks' ability to produce timely data in times of stress.

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

- 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, and streamlining of 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 for each risk type are identified and constructed. Effective measures are put in place to manage customer information and utilise industry taxonomy (eg the LEI).
- 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 have been 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:

- Incomplete long-term IT infrastructure projects aimed at improving data quality and controls by unifying disparate or legacy IT systems.
- 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.
- Weak strategic data architecture or target operating model to help implement the Principles.
- For banks attempting to deploy an integrated IT approach, certain activities from the first and second lines of defence are not fully implemented. 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.
- Inconsistent and disintegrated data dictionaries, data models, data taxonomies and/or definitions. For instance, inconsistent customer codes are used within the bank.
- Inability to produce data and reports under crisis or stressed scenarios highlighted deficiencies in data structure and IT infrastructure.

2 Risk data aggregation capabilities (Principles 3–6)

Supervisors reviewed different types of risk reports to assess banks' data accuracy, timeliness and completeness as well as the adaptability of their risk data aggregation capability to meet 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.

Some supervisors have also explored the use of fire drills to perform ad-hoc assessments of banks' abilities to respond to ad-hoc risk data requests in a timely manner, and the use of 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 clarity on the data content required in a stress situation.

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

- Integrated data taxonomies across the organisation improved data accuracy and quality.
- Proper data quality controls. For instance, there is appropriate data element certification, data quality documentation, data quality assurance mechanisms, assessment of data quality per risk type, and documented and effective controls for manual processes.
- Proper data reconciliation framework across the bank. For instance, there is consistent monitoring and formalisation of reconciliation processes (primarily by providing rationale for differing reconciliation methodologies and results); and reconciliation requirements are established.
- Timely adjustments of risk data aggregation methods and procedures in response to the business development, risks and regulatory changes.

Examples of ineffective risk data aggregation and key compliance gaps:

- Deficiencies in data quality controls. For instance, an inability to map and integrate data quality standards; data quality rules not properly established (eg minimum standards for data quality

reporting thresholds not set); 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.

- A notable presence of manual risk data aggregation processes without proper documentation or manual data amendment policy. Reliance on manual data collection in some cases, especially under stress conditions.
- 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 source risk data from foreign subsidiaries within a short period of time and to automatically aggregate risk data from overseas subsidiaries and institutions due to system constraints.

3 Risk reporting practices (Principles 7–11)

Supervisors assessed risk reporting practices by reviewing reports catering to various levels, including the board, senior management and staff, to ensure that their content, level of granularity and frequency were appropriate.

Bank management would generally identify certain risk reports as critical. Supervisors reviewed these reports to determine whether there was a sharp contrast between the critical reports identified by the senior management and business line managers. Supervisors then ascertained whether these key risk reports were subject to appropriate reviews and reconciliations.

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

- Production of accurate and timely reports in both business-as-usual and ad hoc/stressed situations. The business-as-usual risk reports have certain proactive or dynamic characteristics. For instance, processes are in place to identify changing economic conditions or risks and to adjust reports accordingly. Risk management departments maintain procedures or guidelines for ad hoc reports enabling them to produce consistently accurate and tailored reports for the appropriate audience.
- 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, 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 where specific items have been highlighted for management's attention or action. The reports are also sufficiently detailed in terms of content, enabling the board and/or senior management to make informed decisions.

Examples of ineffective risk reporting by and key compliance gaps at banks:

- Reports are only static in nature and not complemented by more dynamic dashboard-type reporting.
- Overreliance on manual processes to produce reports. These processes also challenged banks' ability to produce reports quickly, in particular ad hoc reports for special requests or crisis situations.
- Challenges to the comprehensiveness of risk reports include:

- Inability to capture sufficiently granular data in certain businesses or areas.
- Inability to monitor emerging trends through forward-looking forecasts and stress tests.
- Incomplete risk reports because of legal constraints preventing banks from gathering data from foreign subsidiaries.

- Challenges to the accuracy of risk reports include:
  - Insufficient controls and inadequate validation rules or procedures.
  - Inadequate procedures to establish identification, reporting and interpretation of data errors.

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

4.1 Supervisory review of banks' compliance

The role of supervisors in the promotion of RDARR capabilities has been continuously enhanced.

Principle 12 states that supervisors should periodically review and evaluate a bank's compliance with the Principles. All supervisors performed risk-specific supervisory activities, using banks' internal audit to evidence levels of compliance, where appropriate.[7] Supervisory activities on RDARR have also been integrated into general supervision programmes and processes. Regular supervisory reviews were conducted by most supervisors as an assessment tool. Apart from these ongoing supervisory activities, some supervisors conducted thematic reviews on RDARR covering multiple banks' compliance with the Principles.

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. Much like the supervision of other activities, supervisors are assessing banks' compliance with the Principles, requiring banks to take remedial action within a specific time frame, requiring independent reviews by a third party, and issuing supervisory letters. Restrictions on banks' behaviours, such as business activities and capital distributions, are potential follow-up measures at supervisors' disposal.

In terms of supervisory process, upon completing any examination activities, supervisors will issue follow-up letters or reports of examination to banks setting out their deficiencies. In response to such letters or examination reports, banks should provide roadmaps to close any implementation gaps. In general, the roadmaps would also describe the types of independent review, such as internal or external audit, to be conducted to assess implementation efforts. In following up on banks' deficiencies, several supervisors would meet with banks' senior management at least quarterly to generally monitor implementation efforts.

Examples of actions which banks were requested to take following risk data examinations:

Governance

- Establishing a board-level committee responsible for data governance, integrity and quality.
- Updating appropriate policies to clearly describe processes for compiling accurate, comprehensive and transparent risk reports.

[7] In many cases, supervisors conducted supervisory activities after banks had completed independent reviews, such as an internal or external audit, assessing hitherto completed risk data implementation activities. Banks were required to submit their audit reports to the supervisors, where the outcomes were factored into the supervisors' assessment.

- Improving reporting of risk data and risk reporting project initiatives, so that these are reviewed with other high-priority strategic initiatives at the bank.
- 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.

Data architecture and IT infrastructure

- Reaffirming the bank's commitment to fund longer-term projects aimed at supporting critical IT infrastructure that will assist the bank in 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 of risk data collection among IT systems.
- For banks looking to acquire other institutions, to consider the entity's RDARR capabilities and issues, and to understand 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 processess and procedures.
- Increasing the number of ad hoc exercises and stress scenarios to produce aggregate risk reports, and developing a framework to 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.
- Developing methodologies to assess the comprehensiveness of risk reports.
- Periodically examining the ability to produce risk reports in crisis or stress situations.
- Stress testing initiatives allowing banks to evaluate the overall effect of credit, market and operational risks under a consolidated stress scenario.

While not targeted specifically at the G-SIBS, a few initiatives may affect their risk aggregation capabilities and could be supported by authorities to foster compliance with the Principles. For instance, two supervisors are promoting the use of the LEI and three are supporting the work on integrated data taxonomies.[8]

[8] 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 and acquisition.

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. In this regard, supervisors are generally satisfied with the existing communication channels through supervisory colleges, crisis management groups, bilateral contacts etc.

Appendix 3: Banks identified as G-SIBs during 2011–16[9]

Jurisdiction	Banks
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
	JP Morgan Chase
	Morgan Stanley
	State Street
	Wells Fargo

[9] 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)
	Tobias Volk	Deutsche Bundesbank
Hong Kong SAR	Polly Cheung	Hong Kong Monetary Authority
Italy	Vicenzo Re Maria	Bank of Italy
Japan	Mitsutoshi Adachi	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 Agency
South Africa	Jacques Henning	South African Reserve Bank
Spain	Cecilia Lozano	Bank of Spain
Sweden	Ken Chen	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
	Eric Gott	Office of the Comptroller of the Currency
European Union	Javier De Diego	European Banking Authority
	Nicola Papa	European Central Bank
Financial Stability Board	Gianmatteo Piazza	Financial Stability Board
	Grace Sone	
BCBS Secretariat	Ethan Goh	Secretariat
	Tamara Gomes	