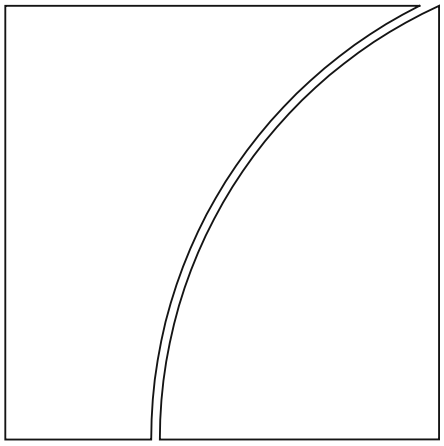
Basel Committee
on Banking Supervision



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

April 2020

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 978-92-9259-377-3 (online)

Contents

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

Executive summary

As of the end of 2018, none of the banks are fully compliant with the BCBS 239 principles, as attaining the necessary data architecture and IT infrastructure remains a challenge for many. In general, banks require more time to ensure that the Principles are effectively implemented.

Nevertheless, banks' continuous efforts to implement the Principles have resulted in tangible progress in several key areas, including overarching governance, risk data aggregation capabilities and reporting practices. Many banks have expanded their implementation scope beyond risk data management to incorporate strategic initiatives, including regulatory reporting, financial reporting and recovery and resolution planning, into their BCBS 239 implementation programmes.

Going forward, banks should continue to closely monitor their BCBS 239 implementation programmes, adapting them as necessary to take into account changes in the financial sector. Banks that have struggled to implement the Principles should address weaknesses promptly, which may include committing the resources needed to complete data architecture and IT infrastructure improvement projects.

Supervisors should continue to monitor the progress made by banks in implementing the Principles. Further, supervisors should take appropriate measures to address delays and ineffective implementation.

1. Introduction

This report outlines the progress made by banks in implementing the Basel Committee's Principles for effective risk data aggregation and risk reporting ("the Principles" or "BCBS 239")[1] based on supervisors' assessments conducted in 2019. Section 1 of this report summarises the background of BCBS 239 and work conducted by the Risk Data Network (RDN)[2] to date. Section 2 gives an overview of banks' implementation of the Principles, provides key observations of supervisors regarding the improvements made and the remaining challenges encountered by banks in implementing the Principles. Section 3 discusses the adoption of the proportionality concept. Section 4 proposes recommendations for banks and supervisors in implementing the Principles.

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

[2] Established under the Committee's Supervision and Implementation Group (SIG) and 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 practice among banks. RDN members meet and exchange information on implementation strategies and supervisory approaches to further implementation of the Principles.

The Basel Committee published the Principles in January 2013 with the aim of strengthening banks' risk data aggregation capabilities and internal risk-reporting practices. Since the publication of this framework, the Committee has been monitoring banks' implementation of the Principles. Between 2013 and 2018, the WGSS and RDN published five reports on banks' progress towards implementing the Principles.[3]

The previous progress report, published in June 2018, highlighted that the implementation progress made by global systemically important banks (G-SIBs) was unsatisfactory. As reported then, a number of banks had encountered delays in fully implementing the Principles, due mainly to the complexity and interdependence of IT improvement projects. Nonetheless, supervisors found that banks had increasingly recognised the value of implementing the BCBS 239 Principles and had accelerated their implementation efforts.

The basis for the present report was a common assessment template, similar to the one used in June 2018, that supervisors of the national jurisdictions completed on banks' progress towards compliance with the Principles. The 2019 assessment exercise, which covered 34 G-SIBs designated during 2011–19 (see Appendix 3), surveyed recent developments at banks and gathered qualitative information regarding the implementation of the Principles as of end-2018. The supervisory assessments form the basis of this report.

2. Assessment results and key observations

2.1 Overview of assessment results in 2019

Supervisors assessed banks' current degree of compliance with each of the risk data aggregation and risk-reporting (RDARR) Principles on a scale of 1 to 4. The four ratings are defined as follows:

- Rating of "4" – *The Principle is fully complied with*: the objective of the Principle is fully achieved within 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-complied with*: 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.

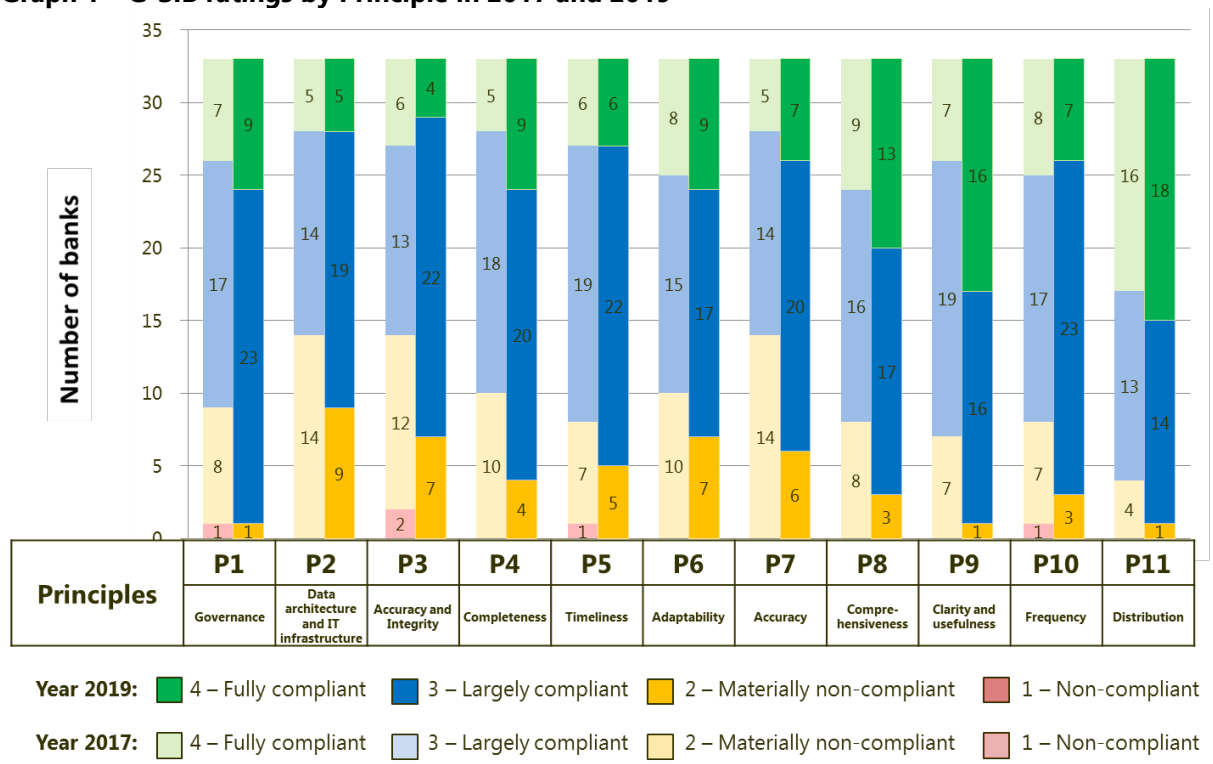
In addition to the ratings, supervisors provided qualitative inputs on the assessment exercise.

2.1.1 Assessment results

The results of the 2019 assessment show that banks have made notable improvements in their implementation of the Principles since the previous assessment. While these efforts are reflected in governance, risk data aggregation capabilities and risk-reporting practices, there is still considerable work ahead for several banks, especially with respect to the further improvement of their data architecture and IT infrastructure.

[3] Please see www.bis.org/publ/bcbs268.pdf (December 2013); www.bis.org/bcbs/publ/d308.pdf (January 2015); www.bis.org/bcbs/publ/d348.pdf (December 2015); www.bis.org/bcbs/publ/d399.pdf (March 2017); and www.bis.org/bcbs/publ/d443.pdf (June 2018)

Graph 1 – G-SIB ratings by Principle in 2017 and 2019[4]



Looking at individual principles, banks generally achieved higher average ratings for all principles in the 2019 assessment. Specifically, more banks obtained the largely compliant or fully compliant ratings (ie ratings of "3" and "4") for all principles. Another positive aspect is that no bank attracted the lowest rating (ie the rating of "1") for any of the principles.

As Principles 1 (governance) and 2 (data architecture and IT infrastructure) lay the foundation for implementing the rest of the Principles, it is of the utmost importance that banks make progress in these two areas. Given the interdependency between the Principles, banks that struggle to fully implement Principle 1 and Principle 2 will also find it challenging to implement Principles 3–11, which cover banks' risk data aggregation capabilities and risk-reporting practices.

Banks made substantial progress in implementing Principle 1, which can be attributed to their efforts in strengthening governance arrangements such as establishing clear ownership and responsibilities for risk data (see Section 2.2.1). Some banks have established independent units for validating risk data management. These functions have reviewed risk data implementation efforts and have reported material weaknesses to the board and senior management.

Meanwhile, as for Principle 2, banks have made improvements to their data architecture and IT infrastructure (eg improved data dictionaries and enterprise data quality metrics), resulting in better ratings. These developments will help banks to satisfy the other Principles, which rely heavily on sound and stable IT architecture. Nevertheless, nine banks were assessed as materially non-compliant with Principle 2, indicating that banks still have much work to do in this area (see Section 2.2.2).

The reasons why banks have been unable to effectively implement Principle 2 have not changed drastically over the years. Banks have unaligned IT solutions and legacy systems, which hamper reconciliations of risk data. This hinders banks in producing accurate reports with sufficient granularity to meet ad hoc data requests. This also explains banks' challenges in implementing Principles 3 (accuracy

[4] To allow a continuous comparison, the graph shows the assessment results of only 33 G-SIBs, excluding the ones newly designated in 2018 and 2019.

and integrity), 5 (timeliness), 6 (adaptability) and 7 (accuracy). Appendix 2 provides more detailed examples of effective and ineffective practices among banks for implementing the Principles.

Despite the improved overall performance, it is noted that no bank was assessed as fully compliant with all the Principles in the 2019 assessment. This contrasts with the 2017 assessment exercise, in which three banks qualified for the rating of "4" for all Principles. Increased awareness among banks has resulted in better in-depth analysis and this, together with the expanded scope of projects aimed at implementing the Principles, partially explains the ratings downgrades.

As pointed out in previous progress reports, implementation of the Principles should be a dynamic or ongoing process. Therefore, banks must reassess their implementation of BCBS 239 whenever there are any key changes in banks' data aggregation processes, business models and risk profiles as well as strategic initiatives (eg mergers and acquisitions).

2.1.2 Expected date of full compliance

With regard to banks' implementation timelines, most banks expect to have implemented the Principles fully or in large part by the end of 2020.[5] Among these banks, some have already begun to transition their initial BCBS 239 implementation practices into their business-as-usual operations, and are in the process of increasing the effectiveness of their implementation practices (see Section 4.1.1).

Table 1 – Expected date of full compliance with BCBS 239

Year	By 2019	By 2020	By 2021	Beyond 2021*
No. of banks	10	13	6	5

* The numbers exclude G-SIBs designated in 2019.

For the banks expected to achieve full compliance after 2020 based on the assessment survey, their primary challenges revolve around their data architecture and IT infrastructure. Banks' IT legacy issues have given rise to fragmented data landscapes, unaligned IT solutions and interdependencies between IT projects, all of which will take considerable time to resolve. Some banks have changed their BCBS 239 implementation strategies, devising comprehensive solutions to address data quality issues rather than seeking a fix via more tactical or ad hoc solutions.

Supervisors should reassess banks' BCBS 239 implementation strategy and update their assessment methods over time. In this light, the ratings given by supervisors are subject to change. In addition, supervisors are gaining experience in assessing banks' implementation of the Principles as a result of the ongoing supervisory activities. As a result, some supervisors have refined their expectations for banks, which may also be a factor in banks' delayed implementation timelines.

2.2 Key observations

While banks have made progress in implementing BCBS 239, several existing and emerging challenges are impeding banks' BSBS 239 implementation efforts.

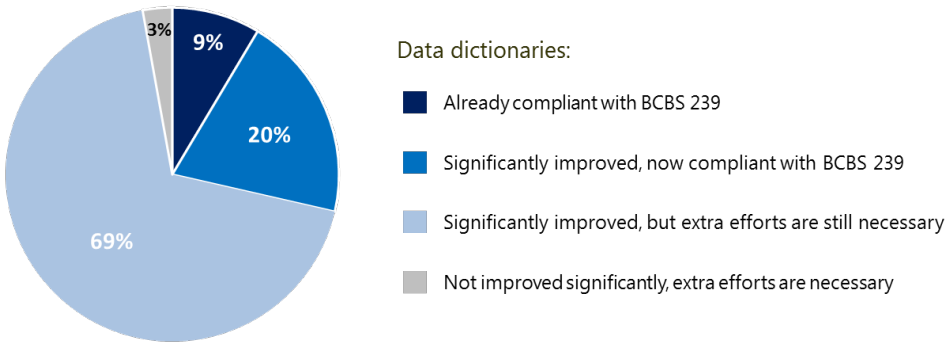
[5] As noted in the *Principles for effective risk data aggregation and risk reporting*, banks identified as G-SIBs in November 2012 should have met these principles by January 2016.

2.2.1 Notable improvements made in a number of key areas

Supervisors observed notable improvements in banks' overarching governance, risk data aggregation capabilities and reporting practices. In particular, banks have:

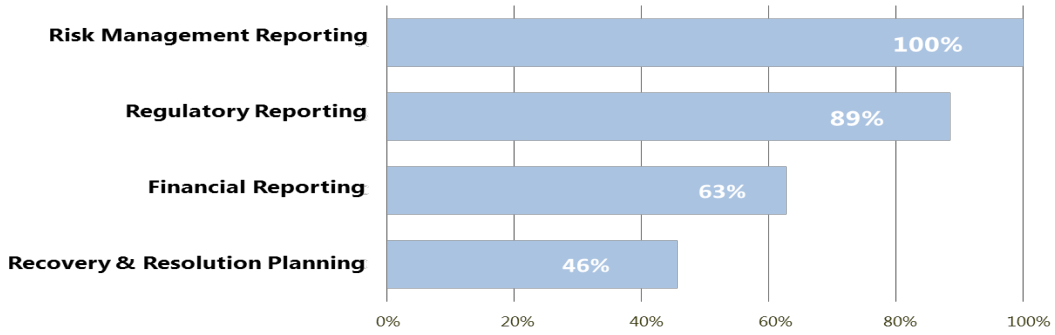
- established enterprise data strategies and data management frameworks, and appointed relevant governance committees and managers for key roles in data management (such as data-owners and -stewards) to improve data oversight;
- improved data dictionaries, which is a key aspect of Principle 3, enterprise data quality metrics and data lineage;
- enhanced quality assurance, allowing identification and correction of data quality issues;
- initiated automated reporting platforms, which strengthen ad hoc reporting capabilities; and
- established group-level reporting policies, which set out the periodicity and dissemination of reports.

Graph 2 – Data dictionaries significantly improved



Supervisors' discussions with banks revealed that many banks have expanded their scope of implementation of BCBS 239 beyond risk management, aligning their BCBS 239 implementation with strategic initiatives such as regulatory reporting, financial reporting and recovery and resolution planning. Graph 3 below shows the different types of reporting that feed into banks' implementations of the Principles.

Graph 3 – Scope of reporting that banks consider when implementing BCBS 239



2.2.2 Existing challenges persisted while new challenges have emerged

While supervisors acknowledge the efforts and improvements made by banks, many banks still have much work to do in fully implementing BCBS 239. In particular, supervisors noted that the aggregation processes of some banks are still not appropriate, in terms of their current capabilities in relation to their size, complexity and activities.

Existing challenges that continue to impede banks' implementation progress include:

- Interdependencies between projects to address IT legacy issues, which may have caused complications and difficulties in systems integration. For example, incomplete or partial IT solutions have hampered progress within ongoing improvement processes for the reconciliation of risk data.
- The scale of banks' operations and structural changes brought by mergers and acquisitions have created complexities in building/harmonising IT infrastructures with the aim of ensuring consistent implementation across the banking group.
- Adapting to one single source for data due to the fragmentation of the data landscape.

In addition to the existing challenges, the evolving and dynamic nature of the banking business presents new challenges:

- In recent years, changes in business and technology have intensified, including developments such as fintech and cloud technologies, compelling banks to upgrade their IT capabilities. This has affected banks' rate of progress in implementing BCBS 239, by increasing complexities and presenting other business and technical challenges.
- Some banks have faced challenges in ensuring data accuracy, timeliness and completeness for outsourced data-related processes against the backdrop of growing use of third-party support for data-related processes.

2.2.3 Supervisory activities in response to the dynamic nature of BCBS 239 compliance

Supervisors generally expect banks to make ongoing enhancements to data aggregation and reporting capabilities as the nature of their activities changes. Supervisory processes to assess banks' implementation of BCBS 239 have also evolved, with supervisors adopting more detailed methods as they gain experience in assessing BCBS 239 compliance. Some supervisors have followed-up with banks on several occasions to monitor whether the agreed roadmaps have been followed. For instance, supervisors have:

- conducted on- and off-site reviews, inspecting banks' management information systems to determine whether they have addressed previously identified data-related issues and if any new issues have surfaced;

- mandated external firms to assess the implementation status of the Principles;
- conducted fire-drills to test the banks' risk data aggregation capabilities;
- increased supervisory intensity in areas where weaknesses have been found; and
- modified assessment approaches to ensure comprehensiveness of the assessment, particularly when banks have modified the scope of BCBS 239 implementation (eg data and reports in scope).

3. Adoption of the proportionality concept

The aim of proportionality is to reflect the relative differences in risk profiles across banks. Given that BCBS 239 is principles-based, proportionality plays an important role both in the implementation of BCBS 239 and in the supervisory assessment of compliance. Primarily, banks are responsible for defining the scope of their compliance with BCBS 239 and for ensuring that their BCBS 239 implementation remains comprehensive and aligned with their business activities, bearing in mind that proportionality should not be applied in a way that undermines the effectiveness of their risk management and decision-making processes.

Supervisory expectations for different aspects or reports that are included in BCBS 239 implementation will vary depending on a bank's size, business model and risk profile, for example:

- In some cases, frequency and timeliness expectations for risk data aggregation and risk reporting are higher for certain risk types such as liquidity and market risks; while such expectations may not be as critical for other risks, such as retail activities.
- The appropriate level of automation for risk data aggregation and risk-reporting processes depends on the volatility of the risk type and other factors. Manual processes in risk reporting can be acceptable provided that the bank has the appropriate mitigants in place (eg end user computing policies and procedures) and other controls that are consistently applied across the bank's processes. However, these manual processes generally become less effective as the complexity or volatility of the risk type increases. This is why banks with more automated risk reporting are better able to implement BCBS 239.

Most jurisdictions also apply a proportionate approach to their supervisory activities, including the intensity level and scope of on- and off-site examinations. Although the Principles apply to all the material risks of a bank, supervisors often adopt a risk-oriented approach and concentrate their assessment activities on the most important risks. Some supervisors choose a staggered multi-year assessment approach and focus more on assessing Principles 1 and 2 as these principles are seen as the preconditions for appropriately implementing the other Principles.

4. Key recommendations

The challenges identified in the past progress reports persist. Therefore, the previously noted recommendations are still relevant. The overarching recommendations from the June 2018 progress report are provided below:

- Banks should continue to implement the Principles in line with their roadmaps and consider how implementation would benefit other initiatives (such as recovery and resolution plans, and financial reporting capabilities[6]).
- Supervisors should maintain supervisory intensity, to ensure that banks implement the Principles, and continue to promote home-host cooperation.

Based on the information obtained from the 2019 assessment, the RDN has identified the following recommendations for banks and supervisors:

4.1 Banks should closely monitor and make appropriate modifications to their BCBS 239 implementation programmes

Banks should monitor their efforts to implement the Principles and make appropriate modifications to governance, IT infrastructure, and data aggregation and reporting capabilities as risks, activities and technologies evolve.

4.1.1 Banks should periodically review BCBS 239 implementation plans to ensure long-term strategic compliance

Appropriately implementing the Principles is an ongoing process because of the evolving and dynamic nature of banks and the banking business. Banks should have monitoring and management information systems in place that provide the boards and senior management with accurate, timely and relevant information to influence and support decision-making and strategic planning. In addition, banks should have forward-looking reporting capabilities to provide early warnings of any potential breaches of risk limits that may exceed the bank's risk tolerance/appetite. The key steps banks should take to implement the Principles effectively include:

- embedding the Principles into their regular risk management activities by regularly assessing the key assumptions, data sources, models, and procedures used in measuring and monitoring risks;
- routinely testing their ability to produce timely and accurate reports;
- regularly simulating capabilities to generate reports during times of stress; and
- incorporating into their BCBS 239 implementation efforts, as appropriate, mergers, new businesses, new technologies, new or modified outsourcing or third-party relationships.

Reviews and assessments of risk data aggregation and risk-reporting capabilities periodically require banks to modify the scope of data and/or reports included in their implementation of the Principles. In these instances, banks should appropriately plan for changes to their BCBS 239 implementation strategy by:

- identifying and prioritising necessary elements (such as the critical data to be covered) for successful implementation;
- modifying previously developed implementation roadmaps when the implementation scope is altered or expanded; and
- taking the necessary steps (such as establishing appropriate mitigating controls for new reports) to ensure existing implementation measures will not be impaired as a result of a change in scope.

[6] For example, the use of industry taxonomy such as the Legal Entity Identifier (LEI) 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.

To integrate BCBS 239 into business-as-usual operations, senior management should promptly report and/or get approval from the bank's board whenever BCBS 239 implementation plans and strategies are modified or delayed.

4.1.2 Banks should promptly and appropriately address weaknesses

Banks that have struggled to implement effective data governance policies, complete IT infrastructure improvement initiatives, and aggregate data should continue to appropriately address these weaknesses.

While many banks continue to make progress in implementing the Principles, others have struggled to implement Principle 2 and other Principles. As previously discussed, one of the primary obstacles in implementing the Principles is the complexity and interdependence of projects to address IT legacy systems. Banks with weaknesses in BCBS 239 implementation should consider:

- promptly addressing supervisory findings from examinations or findings from internal audit or other reviews and processes, and regularly communicating with supervisors to update them on the remediation of findings;
- reviewing and updating implementation roadmaps. Effective roadmaps typically include long-term initiatives rather than tactical or short-term solutions to data quality and data aggregation issues;
- committing the necessary resources to complete IT infrastructure improvement projects and to develop oversight mechanisms for implementing the Principles and identifying areas for improvement; and
- identifying data quality gaps and developing training on improving data quality and implementing the BCBS 239 Principles.

4.2 Supervisors should continue to communicate with banks and inform them if supervisory expectations evolve

Supervisors conduct a variety of activities to assess banks' implementation of the Principles. Supervisors may perform targeted assessments of specific risks, thematic reviews across multiple banks, fire drills or leverage the review of banks' internal and external audit functions.

- Because supervisory approaches to assessing BCBS 239 implementation may vary over time, supervisors should communicate to their banks should there be any changes in regulations or supervisory focus, expectations or BCBS 239 implementation assessment approaches.
- Supervisors should continue to apply the proportionality concept in assessing banks' implementation of the Principles, while making it clear how proportionality is applied to banks.

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.[7]

Principle 2

Data architecture and IT infrastructure – A bank should design, build and maintain data architecture and IT infrastructure that 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 reduce 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 risk exposures, concentrations and emerging risks to be identified and reported.

[7] 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, and will be 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 clearly and concisely. 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 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 set out 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 on how banks have complied with the various principles and deficiencies observed. The following examples are strictly for illustrative purposes and are not meant to be interpreted as guidance on implementation.

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

1.1 Governance

Supervisors have generally used existing supervisory tools or examination methods to assess risk data governance. Some supervisors have devised examination templates or procedures for reviewing a firm's governance of the Principles to promote 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 consider factors such as 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 committees are appropriately empowered to execute the project(s).

Examples of effective governance demonstrated by banks that were rated as fully or largely compliant are:	**Examples of ineffective governance and key compliance gaps of banks are:**
• Policies setting out a clear delineation of roles established and responsibilities for data owners, consumers/producers across the data lifecycle and incentive schemes (eg bonuses and remuneration) linked to the achievement of goals established.	• 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, risk data aggregation and risk-reporting (RDARR) policies are not approved or fully developed across the enterprise or global organisation. • Lack of clarity regarding responsibility and accountability for data quality. • Insufficient authority assigned to staff for the development of a well defined enterprise data programme.
• There is regular independent validation of risk data aggregation and reporting processes. 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.	• Insufficient independent validation.

Examples of effective governance demonstrated by banks that were rated as fully or largely compliant are:	Examples of ineffective governance and key compliance gaps of banks are:
• Integration of risk data governance into overall risk management framework. • Establishment of bank-wide data requirements (eg updated and homogenised internal data governance framework models and policies on data quality). • Inclusion of the board's data quality requirements as part of service level agreements. • Application of Principles to internal reporting, regulatory reporting and financial reporting.	• Plugging gaps in an ad hoc manner, rather than focusing on holistically improving governance capabilities that are consistent with the Principles. • 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 on critical data elements and how those updates should be applied to the overall RDARR framework. • Insufficient data governance approaches. For instance, due to group-level entities' weak involvement, 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. • Insufficiently comprehensive list of risk reports to consider. • Service level agreements for data-related processes are missing.
• Effective and audience-appropriate communication at regular intervals. For example, 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. • There are also open lines of communication among business lines as exhibited by regular interdepartmental meetings on data governance. • Development of new training materials for bank staff.	• Lack of communication on limitations of RDARR practices to key stakeholders. • Training plans need to be improved to enhance awareness of staff in charge of data quality.
• Specific roadmaps with milestones, covering both IT and non-IT plans. • Detailed definition of the key risk indicators, as defined and approved by the board.	• 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.

Examples of effective governance demonstrated by banks that were rated as fully or largely compliant are:	Examples of ineffective governance and key compliance gaps of banks are:
	• Lack of transparent status, progress, and cost reporting to inform key stakeholders of implementation progress. • Inadequate technical expertise on project teams, making it difficult to inform governance committees, thereby creating delivery or decision bottlenecks.

1.2 Data architecture and IT infrastructure

Supervisors continue to review banks' data architecture and IT infrastructure with regard to risk data implementation. Examples include reviewing specific metrics in data architecture for RDARR purposes (eg the proportion of key risk measures available on reporting dashboard), communicating with IT staff to gain insight into banks' data architecture and IT infrastructure (eg the participation of IT examination staff in risk data-specific assessments) and assessing banks' ability to produce data in times of stress. Some supervisors also reviewed the work completed by the bank's internal audit function, and tracked progress on the remediation of issues on an ongoing basis until they are resolved. This exercise also allowed supervisors to validate the adequacy of 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:	Examples of ineffective data architecture and IT infrastructure and key compliance gaps of banks are:
• Allocation of appropriate resources to effectively integrate previously isolated databases from disparate legal entities, subsidiaries and branches. • Projects on data quality assessments and data remediation have been conducted across all business units, sometimes with the use of scorecards. •	• Failure to complete IT infrastructure projects, resulting in the continued use of disparate data warehouses or legacy IT systems that generate poor data quality and aggregation possibilities. • Lack of comprehensive IT strategies including an allocation of financial and human resources.
• 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)).	• Inability to integrate data taxonomies and architecture from some 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. • Lack of data dictionaries for certain risk types, such as operational risk.
• Identification of redundant or inefficient technologies and processes, streamlining IT platforms and systems.	• Lack of appropriate processes and controls to ensure that the risk reference data is updated following changes in

Examples of effective data architecture and IT infrastructure demonstrated by banks that were rated as fully or largely compliant are:	Examples of ineffective data architecture and IT infrastructure and key compliance gaps of banks are:
	• business activities and a lack of a formalised escalation process to communicate poor data quality to senior management. • Dependence on manually intensive processes or end user computing for most routine risk reports and ad hoc reports without sufficient controls/audit trail or adequate testing of manual controls.
• 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.	• Certain activities from the first and second lines of defense are not fully implemented, hindering banks from deploying an integrated IT approach. As a result, an end-to-end ownership model is lacking for critical data throughout the data lifecycle to enable ongoing data oversight and remediation.

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 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 exercises) were also assessed.

Some supervisors have also explored the use of fire drills to perform assessments of banks' abilities to promptly respond to ad-hoc risk data requests, 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 both normal and stress situations.

Examples of effective risk data aggregation demonstrated by banks that were rated as fully or largely compliant are:	Examples of ineffective risk data aggregation and key compliance gaps are:
• Implementation of IT capabilities to aggregate 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.	• Notable presence/overreliance on manual risk data aggregation processes without proper documentation and manual data amendment policy. • Lack of progress due to dependence on strategic IT systems being rolled out.

• Integrated data taxonomies established across the banking group.	• Reference data are insufficiently standardised for risk aggregation and reporting by risk and finance functions. • System constraints prevent bank from promptly sourcing risk data from foreign subsidiaries and automatically aggregating risk data from overseas subsidiaries and institutions.
• Effective data quality controls. For example, there is in place an appropriate data element certification; data quality documentation; data quality assurance mechanisms 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.	• 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.
• Efficient data reconciliation framework across the bank. For example, there is a consistent monitoring and formalisation of reconciliation processes (primarily by providing 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.	• Lack of reconciliation for certain key reports (eg reconciliation between risk and finance data).
• Timely adjustments of risk data aggregation methods and procedures in response to the business development, risks and regulatory changes.	• No variance analysis to determine if there are any changes in reports over time.

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 catered to various audiences including the board, senior management and staff to ensure the content, level of granularity, and frequency were appropriate. In some cases, supervisors carried out fire-drill exercises to assess the ability of banks to accurately and comprehensively report selected data points under a tight deadline.

Examples of effective risk-reporting practices demonstrated by banks that were rated as fully or largely compliant are:	Examples of ineffective risk reporting and key compliance gaps of banks are:
• The business-as-usual risk reports have certain proactive or dynamic characteristics, which support the analysis of various risk types and trends allowing users to analyse risk data more effectively.	• Reports are static in nature and not complemented by more dynamic dashboard-type reporting
• Most of the reports are automated with clear and reliable source data. Manual reports are either in the process of being automated, or contain appropriate controls to ensure report accuracy.	• Overreliance on manual processes or inadequate controls over manual processes to produce reports.
• Critical reports are subject to independent validation.	• Insufficient controls and inadequate validation rules or procedures over risk reports. Processes to report and remediate data quality errors in risk reports are not embedded in the daily business processes.
• Production of accurate and timely reports in both business as usual and stressed situations. • Risk reports feature early testing using scenario analysis, stress test and risk management measures. • When appropriate, banks have also standardised "top of the house" reporting, resulting in consistent identification and communication of risk trends. • The board and senior management have taken steps to identify the scope of data necessary to deal with crisis situations and prepare report templates for the data in advance.	• Risk reports do not contain information on forward-looking forecasts and stress tests, hampering users' ability to monitor emerging trends.
• Risk reports cover all material risk types (eg credit, market, operational, liquidity, reputational, IT and country risks) as well as material concentrations in key industries, products, or geographies. • The reports are also sufficiently detailed in terms of content, enabling the board and/or senior management to make informed decisions.	• Risk report data are not sufficiently granular 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). • Risk reports are incomplete due to legal constraints preventing banks from gathering data from foreign subsidiaries. • Different regions and countries sometimes have different risk packs and risk measures with core metrics that are not fully aligned.
• A unified and controlled 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 confidentiality of risk reporting is appropriately secured through information system controls and encryption.	• Risk reports contain inaccuracies because included data are outdated due to complex processes to aggregate risk data and the time taken to approve the reports.

Examples of effective risk-reporting practices demonstrated by banks that were rated as fully or largely compliant are:	Examples of ineffective risk reporting and key compliance gaps of banks are:
• Risk management departments maintain procedures or guidelines for ad hoc reports enabling them to produce consistently accurate and tailored reports for the appropriate audience.	
• Risk management reports are appropriately tailored to the audience and properly distributed to the relevant internal parties (inter alia board of directors and senior management) and external regulatory authorities.	

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 assessments from the banks' internal audit function or external auditors 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 general, the supervision of banks' implementation of the Principles mimics the supervision of other activities. In terms of the supervisory process, upon completing any examination activities, supervisors will issue follow up letters or examination reports to banks explaining deficiencies. In response to such letters or examination reports, banks should highlight in their roadmaps how such implementation gaps (if any) would be closed. Some supervisors have raised concerns about the slow implementation progress at banks and informed them that the overall supervisory review will consider their level of compliance with the Principles, meaning that insufficient progress could result in Pillar II capital add-ons and/or other measures.

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. Restrictions on banks, such as limiting business activities and capital distributions, are potential follow-up measures at the disposal of several supervisors.

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 at the bank.
- Adjusting the scope of risk data project plans, such as migrating from tactical solutions to longer-term strategic solutions.
- Increasing the scope and capabilities of the independent validation function.
- Developing plans to reduce 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 for bank staff and senior management on 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 implementing the Principles.
- Updating data standards and ensuring that they are applied to the business lines and overseas subsidiaries.
- Increasing the level of automation among risk data collection in IT systems.
- 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 an acquisition on risk data and relevant IT systems.

Data aggregation

- Working with host supervisors of the bank's subsidiaries to receive permission to gather appropriate risk data.
- Ensuring appropriate resources are allocated for managing and implementing risk data aggregation processes and procedures.
- Implementing a framework for producing ad hoc reports and increasing the number of ad hoc exercises and stress scenarios to produce aggregate risk 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 involve establishing a plan to include regulatory reporting into the overall BCBS 239 framework.
- Developing methodologies to assess the comprehensiveness of risk reports.

- Periodically examining the ability to produce timely and accurate risk reports in crisis or stress situations.
- Conduct stress-testing initiatives to evaluate the overall effect of events on key risks, eg credit, market, operational and liquidity risks.

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 between 2011 and 2019[8]

Jurisdiction	Banks
Canada[9]	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[10]
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

8 Dexia is undergoing an orderly resolution process.

9 The Toronto-Dominion Bank, which was designated as a G-SIB in November 2019, has been excluded from analysis in this report.

10 Nordea changed domicile and from 1 October 2018, the bank is domiciled in Finland. Nordea was removed from the FSB list of global systemically important banks (G-SIBs) in November 2018.

Appendix 4: Members of the Risk Data Network

Chair: Sunny Yung[11] (Hong Kong Monetary Authority)

Canada	Bill Rigakos	Office of the Superintendent of Financial Institutions
China	Guangyu Zhang	China Banking and Insurance Regulatory Commission
France	Pascal Jourdain	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
	Naofumi Yamamoto	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
European Union	Nicola Papa	European Central Bank
Financial Stability Board	Gianmatteo Piazza	Financial Stability Board
	Grace Sone	
BCBS Secretariat	Puneet Pancholy	Secretariat

[11] Mr Sunny Yung was RDN chair until 10 January 2020.