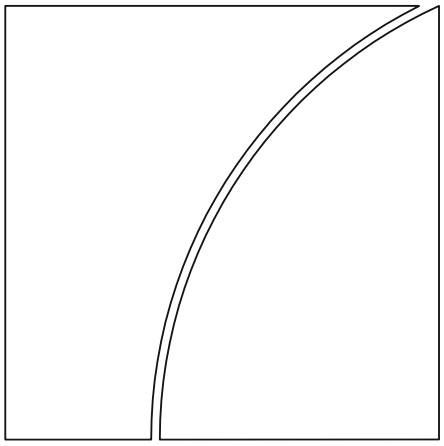
Basel Committee
on Banking Supervision



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

November 2023

BIS

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

ISBN 978-92-9259-712-2 (online)

Contents

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

Executive summary

Nearly ten years after the initial publication of the BCBS 239 principles and seven years after the expected date of compliance, banks are at different stages in terms of aligning with the Principles. Additional work is required at all banks to attain and/or sustain full compliance.[1] The global pandemic and recent stress events provided a stark reminder that banks' ability to manage risk-related data is essential for sound decision making. Of the 31 banks assessed, only two banks are fully compliant with all the Principles. Also, there is not a single Principle that has been fully implemented across all banks.

Although many banks have responded positively to the recommendations of the previous progress reports by establishing adoption programmes and roadmaps to achieve full compliance with the Principles, these programmes were often underfunded, limited in scope and lacking sufficient attention from boards of directors (boards) and senior management.[2] Moreover, several banks failed to fully assess the complexity and interdependence of related projects, especially to address IT legacy systems and set ambitious timelines. Consequently, the recommendations to banks that were identified in the previous reports persist. In addition, bank boards should take full responsibility for overseeing the development, implementation, and maintenance of robust data governance frameworks. Furthermore, banks should foster a culture of ownership and accountability for data quality across the organisation, apply the Principles comprehensively in a broader context and ensure sound data quality as the foundation for digitalisation projects.

The delays in fully adopting the Principles are further exacerbated by the diversity of banks' global operations, their evolving business models and activities, as well as the need for more granular, high frequency data. Additionally, many banks have expanded the scope of their adoption programs beyond risk data aggregation to include more entities and emerging risks, as well as financial and supervisory reporting activities. These changes have led to extended implementation timelines for full compliance. Furthermore, the global pandemic and other recent stress events brought into greater focus the known and newly identified weaknesses/ challenges at banks with fragmented IT landscapes and deficient risk data aggregation and reporting capabilities.

To assess banks' adoption of the Principles and to address identified deficiencies, supervisors continue making use of a broad range of supervisory activities and measures. Given the significant work remaining at most banks to fully adopt the Principles, the recommendations to supervisors that were highlighted in previous reports still apply. In addition, supervisors should consider making greater use of the more intensive targeted activities (eg onsite inspections, deep dive reviews or fire drills), applying more forceful measures to address long-standing risk data aggregation and reporting deficiencies (eg capital add-ons, restrictions on capital distributions and other penalties/fines), and encouraging the application of the Principles in a broader context.

[1] While this report uses the term "compliance" with respect to the Principles, not all jurisdictions actually require compliance with the Principles since certain jurisdictions did not transpose them into their national framework. Notwithstanding that, all jurisdictions support the adoption of the Principles.

[2] The terms "board of directors" and "senior management" are used mainly from the perspective of a one-tier board structure. Certain jurisdictions have different types of governance structures. These terms should therefore be interpreted throughout the report in accordance with the applicable law within each jurisdiction.

1. Introduction

The Great Financial Crisis that began in 2007 revealed that banks' information technology and data architectures were inadequate to support the broad management of financial risks. In response, the Basel Committee on Banking Supervision (Committee) published the BCBS 239 Principles for effective risk data aggregation and risk reporting (Principles)[3] 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' adoption of the Principles. Between 2013 and 2020, the Committee published six reports on banks' progress towards full implementation.[4]

Despite banks' continuous efforts to implement the Principles, some banks are still struggling with the adoption. According to the last progress report, published in April 2020, none of the assessed banks were fully compliant with the Principles. Also, the Financial Stability Board's (FSB) March 2021 Too-Big-To-Fail evaluation report[5] identified gaps in the field of risk data aggregation and noted that banks need to improve their risk data aggregation and reporting frameworks.

The following report provides an update on the progress made by 31 G-SIBs (designated during 2011-2021) (see Appendix 2 for list of G-SIBs) in adopting the Principles. Much like the previous reports published in June 2018 and April 2020, this report is based on a common assessment template that supervisors of the individual jurisdictions completed based on data as of June 2022. Recognising the dynamic nature of the topic in scope, the new assessment template incorporates questions to capture the relevant emerging trends and recent events (eg Covid-19 pandemic, Archegos incident or the Russia-Ukraine conflict), as well as a "case studies" section for supervisors to share experiences on banks' practices and challenges in implementing the Principles. In addition to the assessment template, an outreach session with subject matter experts from selected G-SIBs was organised in March 2023 to augment the insights gathered through the assessment template.

The report is divided into two main parts. The first part of the report looks at banks' progress in adopting the Principles by comparing the 2022 assessment with previous assessments, highlighting notable improvements, remaining key challenges, activities, and recommendations to banks for implementing the Principles. The second part of the report focuses on supervisory approaches and provides an overview of supervisory activities and measures to oversee and promote the adoption of the Principles, complemented by recommendations to supervisors for furthering these efforts. Appendix 1 of the report contains a set of case studies illustrating certain banks' practices and challenges in implementing the Principles. The report exclusively comprises anonymised data and refrains from employing or alluding to any confidential bank information.

2. Banks' adoption of the Principles

2.1. Overview of assessment results in 2022

Supervisors assessed banks' current degree of compliance with each of the Principles on a 1 to 4 scale. The four ratings are defined as follows:

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

[4] Please see https://www.bis.org/publ/bcbs268.pdf (December 2013), https://www.bis.org/bcbs/publ/d308.pdf (January 2015), https://www.bis.org/bcbs/publ/d348.pdf (December 2015), https://www.bis.org/bcbs/publ/d399.pdf (March 2017), https://www.bis.org/bcbs/publ/d443.pdf (June 2018) and https://www.bis.org/bcbs/publ/d501.pdf (April 2020).

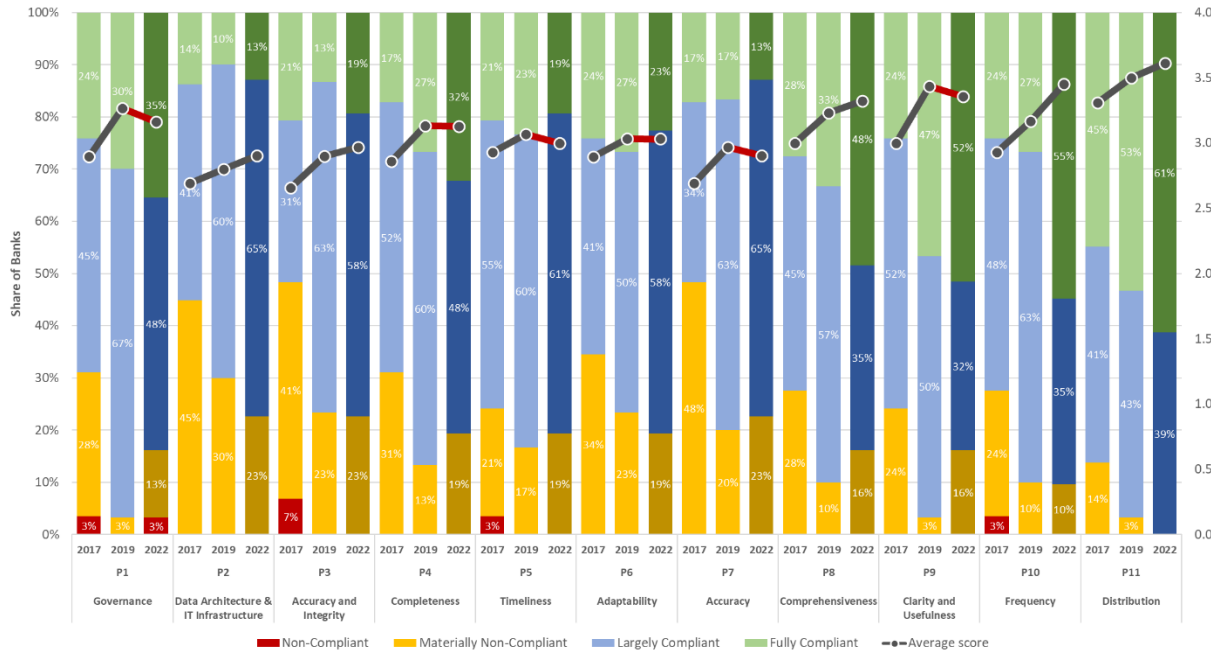
[5] See https://www.fsb.org/wp-content/uploads/P010421-1.pdf.

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

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

Graph 1 shows the assessment results for the banks in the sample for 2022 and compares them with the results of the previous progress reports. The vertical columns in the chart show the relative percentage of banks' compliance ratings per Principle while the lines with markers show the average compliance rating across all banks per Principle.

Graph 1: Bank compliance ratings by Principle in 2017, 2019 and 2022[6]



The 2022 compliance assessment shows that nearly ten years after the initial publication of the Principles and seven years after the expected date of compliance, banks are at different stages in terms of aligning with the Principles, and that additional work is required at all banks to attain and/or sustain full compliance. While most banks have achieved the rating of largely compliant (ie rating of "3") or fully compliant (ie rating of "4") across Principles. Of the 31 banks assessed, only two banks are fully compliant with all the Principles. Also, there is not a single Principle that has been fully implemented across all banks.

In comparison to the 2017 assessment, the 2022 assessment shows a general improvement of the compliance ratings on an aggregated level across Principles. This is best illustrated by the average compliance rating (Graph 1, right axis). The improvements since 2019, however, are mixed and therefore

[6] Due to newly designated G-SIBs in 2017 and 2019 the number of banks that were covered in the assessment varies between the different years (2017: 29 banks, 2019: 30 banks, 2022: 31 banks).

are less evident on an aggregate basis. Furthermore, for some Principles the aggregated compliance rating has even deteriorated from 2019 to 2022.

As illustrated in Graph 1, the 2022 assessment shows an increase in the percentage of banks that fully comply (ie rating of "4") with Principles 1 (governance) and 2 (data architecture and IT infrastructure), which lay the foundation for implementing the remaining Principles. However, the average compliance rating for Principle 1 reveals a slight deterioration from 2019 to 2022 on an aggregated level. This is caused by an increase in the number of banks that are materially non-compliant (ie rating of "2"), with one bank even receiving the lowest rating (ie rating of "1") for Principle 1, a deterioration from its previous assessment.

Similarly, for Principles 5 (timeliness) and 7 (accuracy of risk reports) the average compliance ratings have deteriorated from 2019 to 2022, while for Principles 4 (completeness), 6 (adaptability) and 9 (clarity) the average compliance ratings remained rather stagnant. This observation is largely attributed to the greater percentage of banks that received a materially non-compliant rating (ie rating "2") in 2022 compared with 2019. There were also fewer banks rated fully compliant (ie rating "4") for Principles 5, 6 and 7 in 2022 compared with 2019.

It should be noted that the observed variations in the adoption progress might also be explained by changes in the intensity of supervisory activities in certain jurisdictions (eg use of more intrusive supervisory approaches like onsite inspections, risk specific reviews and/or deep dive exercises) and additional information on weaknesses and/or challenges in banks' risk data aggregation and reporting capabilities as revealed by the pandemic and other recent stress events.

2.2. Key observations

2.2.1 Notable improvements made in key areas

Supervisors observed improvements in the overarching governance, risk data aggregation capabilities and reporting practices of several banks in comparison to the April 2020 adoption report, which have positively affected their compliance ratings.

From a governance perspective, supervisors note that a few banks have made progress in implementing mature enterprise data management frameworks, appropriate committee oversight and end to end ownership, accountability, and monitoring of data throughout the data lifecycle. Some banks have also developed well documented policies and procedures that regulate how IT/data processes (ie data quality criteria and controls, meta data management, data models, etc) should be implemented and enforced. Also, banks increasingly engage in ongoing assessment and independent validation of their data management practices, including progress in implementing the Principles. See section on "governance arrangements" in Appendix 1 for selected case studies).

With regard to risk data aggregation capabilities and reporting practices, some banks managed to simplify their IT landscapes through material reduction in IT systems and applications, harmonisation of IT systems between local entities and the banking group and the use of central data repositories and monitoring tools. In some cases, banks are also introducing cloud computing that helps to improve continuity and compatibility of applications, security and performance. Some banks are implementing automated reporting platforms and business intelligence tools for on-demand creation of customisable reports and analysis. Supervisors also observe a growing use of data quality dashboards that are routinely produced to ensure transparency, reporting and management of data quality issues globally. See sections on "IT infrastructure and data architecture", "risk data aggregation" and "risk reporting" in Appendix 1 for selected case studies.

2.2.2 Key challenges with adoption

The overall pace of banks' progress in implementing sustainable risk data aggregation and risk reporting capabilities is occurring at a slower pace than envisaged. This is largely because several banks have persistent challenges with fragmented IT landscapes, legacy systems and manual processes that are not fit for purpose.

Data architecture and IT infrastructure improvements can take some time to implement due to the complexity of banks' operating environments globally. IT roadmaps affect many domains, business areas and subsidiaries and are often subject to changes or delays. Several banks still lack a common taxonomy and complete data lineage, which further complicates banks' ability to harmonise systems and detect data defects. Also, at certain banks, board and senior management lack awareness/attention to data issues, and therefore do not ensure appropriate budget, resources and accountability for risk data aggregation and reporting initiatives. Additionally, some banks have reassessed or expanded the scope of their initial action plans to adopt the Principles to incorporate recent changes in their business model/ activities or to address known limitations in the entities' data and reporting, resulting in further extension of adoption timelines.

New technologies such as artificial intelligence have not yet materially impacted banks' risk data aggregation and risk reporting processes. While banks regularly emphasise the potential of new technologies to help overcome persistent data management challenges (such as ability to automate documentation, reduce manual interventions, automate the discovery and visualisation of data flows, and maintain data lineage), many banks still lack quality data, which is a prerequisite for embarking on any digitalisation project.

The global pandemic and other recent stress events have further highlighted that stress situations, where data are often required to be tailored to the specific circumstances and reported at a higher frequency, can be a strain on banks' IT systems, requiring some banks to re-design and/or simplify certain internal processes. These events further emphasised the importance of standardisation and automation of data governance /management processes across banking entities, businesses, and functions, as well as the need for sophisticated risk reporting systems, for managing through unexpected events and novel challenges. See section on "risk reporting" in Appendix 1 for selected case studies.

Furthermore, supervisors note that even banks that are more favourably aligned with the Principles experience some challenges. In fact, sound data governance/management processes require continuous improvements to keep pace with changing business strategies, new technologies, external developments, evolving regulatory requirements, and changing customer and counterparty behaviour. As many banks recognise that data is an asset, they continue to work on improving their IT infrastructures, establishing a common taxonomy, and completing data lineage to make data more useful and valuable.

2.2.3 Activities to address key adoption challenges

Recent stress events compelled banks to take or to plan actions aimed at overcoming the difficulties encountered in managing risk-related data. Notably, these actions differ from bank to bank. This variety of approaches is positive, as supervisors recognise banks' specificities and therefore encourage banks to use different paths in adopting the Principles and are not looking for convergence to a single approach.

In relation to their overarching governance and infrastructure, banks are mostly updating data policies, procedures and standards as well as expanding the scope of entities and data (eg risk management data, regulatory data and financial data) subject to the enterprise-wide data warehouse. Additionally, some banks have reported the rollout of specific training initiatives, thematic audits, and validation activities pertaining to risk data aggregation and reporting.

To improve risk data aggregation capabilities, several banks are focusing on internal control enhancements and the improvement of automation in the data aggregation process, including expanding

the scope of entities or transactions subject to automatic data linkage. Banks are also highlighting the value of conducting fire drills to analyse any deviation from planned actions and to identify successful practices in stress situations.

Banks have taken specific actions to improve their risk-reporting practices following the global pandemic and other recent stress events. In particular, banks initiated projects to increase data granularity and improve their ad-hoc reporting capabilities (eg taking transaction level data from source systems of local entities instead of receiving aggregated data). This allows for more flexibility in data aggregation to create specific data views for internal and external stakeholders. Furthermore, integrated reporting solutions have been adopted or are planned to give more flexibility in analysis and ensure automated distribution and a full audit trail. Several banks are also working on the automation of critical reporting processes to minimise manual interventions and ensure reliable data. To identify additional areas for improvement some banks make use of regular surveys among data users.

2.3. Recommendations to banks

As noted in the overview, the assessment of banks' adoption of the Principles reveals that banks are at different stages in terms of aligning with the Principles. While some are already fully or largely compliant, others still have significant room for improvement.

The delayed compliance with the Principles is largely attributed to lack of prioritisation, insufficient ownership by the board and senior management, as well as challenges with implementing data architecture and IT Infrastructure improvements. This may be due to the diversity of G-SIBs' operations globally, their evolving business models and activities, and the need for more granular, high frequency data. Many banks have expanded the scope of their adoption programs to include more entities and emerging risks, as well as regulatory and financial reporting.

The global pandemic and recent stress events provided a stark reminder that banks' ability to manage risk-related data is essential for sound decision making. Banks with fragmented IT landscapes and deficient risk data aggregation capabilities have difficulty providing board and senior management with timely, accurate and complete information to manage the risks of their organisations. Supervisors note that some banks encountered difficulty adapting their reporting processes in response to regulators' requests for granular, ad hoc information at an increased frequency and had to revert to resource intensive manual reporting processes that may not be sustainable for prolonged periods of stress or during an economic downturn.

Notably, the 2022 assessment also reflects some divergence with banks' perception of their adoption of the Principles, which tended to be more positive than that of their respective supervisor. Supervisors note an interesting dichotomy where certain banks consider themselves to be "fully compliant" with the Principles (in some cases, several cycles ago) while they continue to struggle with systemic data quality issues with multi-year remediation programs underway to address them. In those cases, most banks viewed the Principles as being narrowly defined compared to the broader data issues that they experience. In addition, it is worth highlighting that the adoption of the Principles is not a static process and must be assessed by banks on an ongoing basis, due to the constantly evolving and dynamic nature of banks and banking activities.

Based on the information obtained from the 2022 assessment, the following additional recommendations to banks were identified.

2.3.1 Banks should continue to implement the recommendation of the previous reports.

Although many banks have responded positively to the recommendations of the previous progress reports by refining their adoption programmes and roadmaps to achieve full compliance with the Principles, these programmes were often underfunded, limited in scope and lacking sufficient attention from board and

senior management. Moreover, several banks failed to fully assess the complexity and interdependence of related projects, especially to address IT legacy systems and set ambitious timelines.

Consequently, the recommendations to banks that were identified in the previous reports remain applicable:

- 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).
- Banks should periodically review BCBS 239 implementation plans to ensure long-term strategic compliance.
- Banks should promptly and appropriately address weaknesses.

2.3.2 Bank boards should prioritise and intensify their oversight of data governance, including the development, implementation, and maintenance of robust data governance frameworks, risk data aggregation and reporting.

A key success factor for implementing the Principles is strong board and senior management ownership. Alignment with the Principles should be a top priority for banks, and the board of directors should formulate their expectations for senior management to meet this requirement. The board of directors should assume a proactive role in overseeing the adoption of the Principles, including the development, implementation, and maintenance of a robust data governance framework that includes effective risk data aggregation and reporting throughout the bank. The framework should outline a clear separation of senior management's roles and responsibilities for risk data aggregation and reporting across the three lines of defence as well as include stipulations of roles and responsibilities for the board of directors and its subcommittees.

2.3.3 Banks should foster a culture of ownership and accountability for data quality across the organisation.

Banks should establish distinct ownership and accountability for data quality by designating data owners, as well as independent units for validating risk data and risk reporting and foster a data culture across the organisation. Banks should formulate and present a standard set of key performance indicators (KPIs) to the board of directors that allows them to assess data quality for all material group-level risks.

2.3.4 Banks should apply the Principles comprehensively to risk data in a broader context.

The BCBS 239 framework should have a clearly defined scope of application that allows institutions to identify, monitor and report exposure to risk. The scope should be well documented and specify the reports, models and indicators that are included. It should be comprehensive and include, at a minimum, all main risk reports for all material risks. All business processes should be covered (front to back) and the full data lifecycle from data origination, capture, and aggregation to reporting, should be reflected. The scope should cover all material legal entities, business lines, and risk, financial, and supervisory reporting activities.

2.3.5 Banks should ensure sound data quality as the foundation for digitalisation projects.

New technologies may help banks to address persistent challenges such as the ability to automate documentation, reduce manual interventions, automate the discovery and visualisation of data flows, and maintain data lineage. However, before embarking on any digitalisation project, banks should ensure the quality of source data, which is commonly recognised as the root cause for either good or poor outcomes downstream. Common data taxonomies and other tools to enhance consistency in data standards may help in this regard. Equally important is the design and maintenance of data lakes with a high degree of

scalability and adaptability that serve expanding and multiple needs of both internal and external stakeholders.

3. Supervisory approaches in response to the dynamic nature of compliance with the Principles

3.1. Overview of assessment results in 2022

3.1.1 Supervisory activities for adoption assessment

Supervisors continue to make use of a variety of activities to assess banks' adoption of the Principles.

- Onsite examinations enable inspectors to conduct in-depth and comprehensive assessments, gain insights for identified weaknesses, and seek evidence for concrete adoption.
- Deep dive exercises and risk-specific reviews are used for focused/in-depth assessment on specific topics.
- Fire drills are adopted in some jurisdictions to test banks' ability to aggregate and report risk data under simulated stress scenarios or events.
- Self-assessments, continuous supervision and offsite reviews are typically used as on-going tools to support other supervisory activities for generating insights. Banks' self-assessments, while needing to be validated, provide a basis for the supervisory assessment and remediation activities. Continuous supervision is often used for monitoring and/or keeping up pressure on banks' adoption progress, while offsite reviews are a useful tool for benchmarking.
- In a few jurisdictions, supervisors collaborate with external auditors.

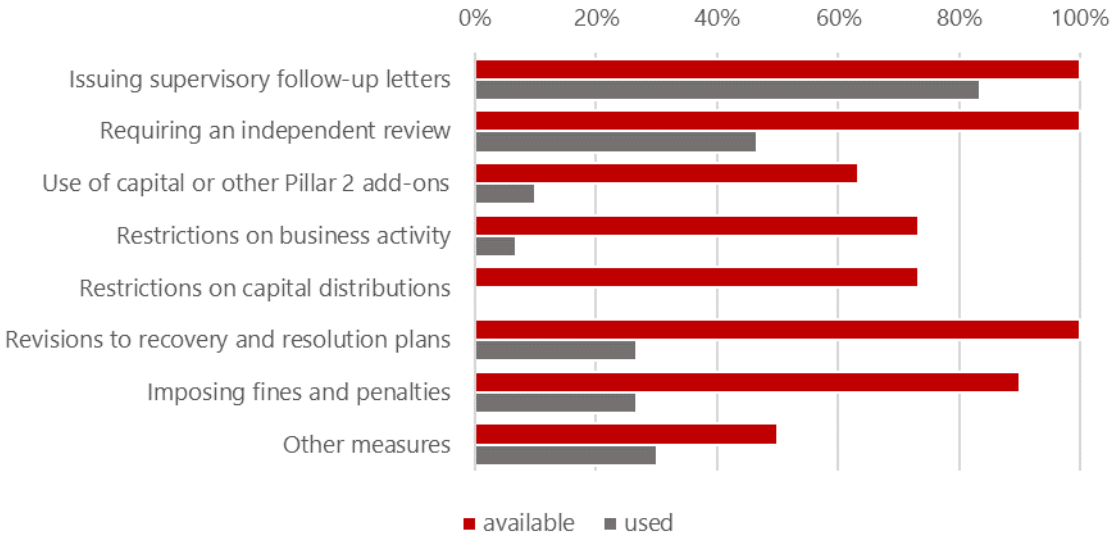
Supervisory assessments of banks' progress in adopting the Principles are often based on the review of internal management and regulatory reports, which are the primary means of identifying and reporting risk exposures, concentrations, and emerging risks for many banks. Financial reports, recovery and resolution plans, and budget and forecasting information are also reviewed by some supervisors, as many banks have expanded the scope of their BCBS 239 programs to areas other than risk data reporting. Other supervisors go even a step further and focus on broader data and risk management, of which Principles related activities are only a subset.

3.1.2 Supervisory measures for addressing banks' deficiencies and their communication

Supervisors have a variety of measures in place for addressing deficiencies identified in banks' risk data aggregation and risk reporting practices. Graph 2 compares the availability and usage of each of these measures for the banks in the sample.

Two commonly used measures are supervisory follow-up letters (on findings from supervisory activities) and mandated independent reviews by banks. Measures which carry a significant impact on banks (eg restrictions on capital distributions or business activities, capital or other Pillar 2 add-ons), by contrast, are only very rarely utilised, despite the lack of progress by several banks. Other measures mainly refer to an increased supervisory oversight.

Graph 2: Availability and usage of supervisory measures



In terms of communication with banks, supervisors often revert to a written report, follow up letter or meeting to convey supervisory expectations, BCBS 239 assessment results, and to determine follow-up actions. While alternative forms of communication such as collective meetings with multiple banks and public reports are possible, they are not commonly used, partly because of individuality and confidentiality regarding the adoption status of the Principles.

3.1.3 Impact of recent stress events and emerging trends

The heightened supervisory monitoring and data collection activities established during the global pandemic as well as recent stress events served as an opportunity for supervisors to observe banks' risk data aggregation and risk reporting capabilities (eg in terms of data accuracy, timeliness and adaptability) in near real time. The gained insights confirmed known issues and/or challenges with banks' risk data aggregation and risk reporting and in certain cases revealed new aspects.

Supervisors generally acknowledge the need for continued improvement in banks' data architecture and IT infrastructure and try to incorporate these topics into their supervisory coverage. In fact, several jurisdictions address risk data aggregation and risk reporting issues in the broader context of "data governance" or "risk management". Also, the impact of new technologies on banks' risk data aggregation and risk reporting processes is carefully monitored and assessed to determine if adjustments to the supervisory approaches are necessary.

3.2. Recommendations to supervisors

The assessment of supervisory approaches shows that supervisors continue making use of a variety of activities to assess banks' adoption of the Principles, and make adjustments as necessary during periods of stress or to address emerging trends such as new technologies. While there is a variety of measures supervisors can choose from for addressing deficiencies identified in banks' risk data aggregation and risk reporting practices, they largely rely on less forceful measures.

Based on the information obtained from the 2022 assessment, the following recommendations to supervisors were identified. Supervisors may consider these recommendations in their supervisory process to assist banks in furthering their risk data aggregation and risk reporting capabilities in accordance with the Principles.

3.2.1 Supervisors should continue to implement the recommendation of the previous reports.

Given the significant work remaining at most banks to fully adopt the Principles, the recommendations to supervisors that were highlighted in previous reports still apply:

- Supervisors should maintain supervisory intensity to ensure that banks implement the Principles, and continue to promote home-host cooperation.
- Because supervisory approaches to assessing BCBS 239 implementation may vary over time, supervisors should communicate to their banks 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.

3.2.2 Supervisors should make use of more targeted and intensive activities as a complement to on-going supervision.

To enhance the effectiveness of on-going supervisory activities (ie continuous supervision, off-site review and bank's self-assessment), supervisors should integrate more targeted and intensive activities such as onsite inspections, deep dive exercises or fire drills, as appropriate, into their supervisory approach. Some banks have found regular fire dills useful in preparing them for stressed situations, for instance, concerning how to strike an appropriate balance between timeliness, accuracy, and comprehensiveness of required risk data where ad hoc data may be required within a shorter timeframe and with higher frequency.

3.2.3 Supervisors should consider more forceful measures to address long-standing risk data aggregation and reporting deficiencies.

Currently supervisors primarily use measures such as supervisory follow-up letters and/or mandated independent reviews by banks to address known deficiencies related to BCBS 239. In cases where banks' progress in remediating long-standing significant deficiencies is insufficient, supervisors should consider imposing more forceful supervisory measures (eg capital add-ons, restrictions on capital distributions or business activities, other penalties/fines) to further promote the remediation of banks' deficiencies in risk data aggregation and risk reporting.

3.2.4 Supervisors may encourage the application of the Principles in a broader context.

Deficiencies in risk data aggregation and risk reporting may apply to other data types or may result from general flaws in data governance and data management. Supervisors should therefore not look at risk data aggregation and reporting in isolation. The Principles provide useful guidance that may have application to other kinds of data. Therefore, supervisors may want to encourage and monitor the application of the Principles in a broader context (ie risk management reporting, regulatory reporting, financial reporting, recovery and resolution planning).

Appendix 1: Case studies

As part of the assessment template that supervisors of the individual jurisdictions completed, supervisors were invited to share experiences on banks' practices and challenges in implementing the Principles. From the collected information the following case studies were selected to demonstrate the wide range of practices observed, highlighting the actions taken to overcome challenges faced in adopting BCBS 239.

In each of the four areas covered below – governance arrangements, IT infrastructure and data architecture, risk data aggregation, and risk reporting – key factors for success and key challenges are identified (to varying degrees) across the case studies. It is important to note that all four areas are to a certain extent interconnected. Some case studies are therefore referenced across multiple areas. While each case study is different and has unique elements, there are often common themes or factors that cut across the case studies. For example, the importance of tone from the top and sound data culture are common success factors, while legacy systems, manual processes, the integration of IT systems, increasing costs of sound data management and talent retention / subject matter expertise are recurring challenges. Another factor prevalent among the different case studies is the importance of sound data controls that act as important checks at the different stages of the data lifecycle.

Importantly, the featured case studies do not attempt to indicate whether one bank's approach is preferable to another, especially since each bank employs approaches most suitable to its particular business model and level of complexity. All bank information has been anonymised and there is no confidential or sensitive information included.

Governance arrangements

A strong governance structure is a critical factor for successful risk data aggregation and reporting capabilities (see Principle 1). Each bank may have a different governance arrangement that best fits its unique mix of business activities and organisational structure, but there are several key governance framework attributes that support sound risk data aggregation and broader data governance/management, with a strong commitment from the board and senior management being most crucial. However, a strong governance framework alone cannot surmount other material impediments to aligning with BCBS 239 (eg legacy IT frameworks, manual processes, poor data security, fragmented data systems).

The following case studies show how banks implemented governance arrangements to address existing challenges:

Overarching data governance frameworks

A comprehensive data governance framework with clearly defined roles and responsibilities to manage data and address data quality and other data-related issues is essential for successfully implementing BCBS 239.

One bank has established a group-wide comprehensive data governance framework that includes compliance with BCBS 239. The framework requires board and senior management review and approval to ensure adequate deployment of resources for a successful outcome. The adoption of the framework is overseen by a dedicated group data office, responsible for data governance, data standards, data management and records management, as well as liaising with business data officers and owners of the IT supporting the data structure. The group data office reports to a member of the board, who is ultimately responsible for data quality. In its regular reports to board and senior management, the group data office informs about progress, issues, delays, and functioning of the framework relative to board-approved thresholds to assess effectiveness. To ensure that also business-specific issues can also be considered, business areas regularly report on their data framework status through the governance

structure. As part of the data governance framework monitoring, regular presentations on BCBS 239 adoption status are also provided to the board- level committees.

Within the data governance framework there are also specific BCBS 239 operating committees to monitor progress and adherence to relevant group standards. Group standards cover all aspects of data management ranging from governance to data lineage, data sources and reference data to the required IT architecture. All standards lie in the responsibility of the group data office.

In addition to the group data office, data officers in each business area are tasked with monitoring the adherence to the related standards. This includes the sign-off on key risk data elements for each business area. All functions involved in the framework have defined and approved responsibilities according to their respective roles.

Newly created central risk data systems support the aggregation of data along with controls such as daily reconciliations to supporting systems. Risk data is migrated to these systems on a controlled basis to minimise operational risk. In addition to risk data, supporting information, such as reference data and relevant controls, is included in these systems over all data elements. Full integration of all governance controls is ongoing as legacy systems are retired and manual controls are replaced by automation. The governance structure allows for reporting and monitoring of completed migrations up to and including the executive level, both by risk types and by business areas. The group executives can monitor and adjust the approach as required to ensure the agility of the framework.

End-to-end definition of roles and responsibilities

Another critical element for successful BCBS 239 adoption is establishing clear roles and responsibilities for data quality along the complete (end-to-end) data flow. One bank deployed a governance framework which entails a network of end-to-end data owners to drive standards for data quality and reporting. Within this framework, ownership is designed to drive efforts to ensure good data quality, as data quality is measured and reflected in the assessment of how standards are applied in the respective areas from input to output.

Adoption of the governance framework was set by a realistic and committed plan that includes clear measures and monthly monitoring by a senior steering committee (chaired by the CEO), as well as oversight by the board. The plan prioritises business and support areas at a global level before being deployed to smaller subsidiaries. The framework adoption has led to improvements in data management and data quality monitoring. Every time a data point is used, any doubts about its meaning are resolved by directing the data user to the respective data owner. Similarly, if a data quality problem is detected, the data owner will be responsible for remediation, eg adding the needed data quality rules to meet standards. As the bank was developing the framework, management has clearly demonstrated its commitment to robust governance and monitoring of the project, which has been critical to effective adoption, and the process has raised the bar for data quality across the bank.

Independent validation activities

An independent validation process is an important component of a strong governance framework. One bank has created a dedicated team within the second line of defence to perform independent data validation activities, reviewing the bank's risk, treasury, and finance risk data aggregation capabilities and risk reporting practices. The team's success comes from an agreed mandate between the business lines (first line of defence) and control functions (second line of defence), with the operational processes documented and clear guidance from all sides. The team reviews risk data aggregation aspects such as BCBS 239 scope of risk metrics and reports as well as their respective compliance with the standards. These activities are performed in addition to the regular activities of the internal audit function (third line of defence). The internal audit function also performs regular audits on the risk data aggregation and risk

reporting framework and contributes to maintaining awareness of data quality risks, needed improvements and remaining challenges.

IT infrastructure and data architecture

Besides effective governance arrangements, adequate IT infrastructure and data architecture are paramount for sound risk data aggregation and risk reporting practices (see Principle 2). The following case studies show how some banks approached existing challenges in practice:

Fragmented IT infrastructure

Fragmented IT infrastructure and legacy systems remains the leading challenge for banks to establish sound risk data aggregation capabilities and risk reporting practices. One bank faced a heterogeneous landscape of different data lakes (DLs)[7] across the group, legal entities, businesses, and risk areas. Each DL was managed in a different way and with varying efficiencies that resulted in data that went partially unused or was duplicated. Subsequently, a strategic horizontal project was initiated to understand the magnitude of the issue, define rationalisation plans, streamline the DL landscape to fit it to business use cases and ultimately create cost savings.

As a starting point, the bank created an overview of all DLs across the legal entities and areas (eg risk, business, analytics). The DLs were categorised based on business need and data usage for determining to what extent they could be decommissioned. This approach also considered cost savings and reduced resources associated with decommissioning DLs and the efficiencies gained from increased automation of data quality tasks. The review highlighted that investments in DLs were not necessarily dedicated to business needs, which showed the need for a DL inventory for financial control and tracking the data usage. The bank also created a business use case decision tree, to determine if it is reasonable to use a DL or if it would be better to stick to an existing technology/repository.

The bank encountered many challenges with DL rationalisation particularly at the local level due to regulatory constraints in some countries, lack of budget/priority and subject matter expertise. Subsequently, action plans and remedial actions were developed.

To overcome these challenges and successfully complete the project, the bank's senior management monitored the action plans on a quarterly basis in the executive data committee, chaired by the CEO. Besides the tone set from the top, a key success factor was to place the emphasis on business use cases, which helped to secure buy-in from data stakeholders and local business units. Overall, the project led to DL rationalisation and a significant reduction in data duplication.

Management of evolving data needs and changes in existing IT infrastructure

Banks' risk data aggregation capabilities and the underlying IT infrastructure should be flexible and adaptable to meet ad hoc data requests and to assess emerging risks.

One bank faced a surge of regulatory requirements driven by the Basel III final reform package, growing demand for internal analyses to support executive management decision making and significant increase in external disclosure requirements. The legacy data sourcing, aggregation and reporting processes required significant manual intervention and end-user compensating controls to ensure reports and analyses were complete, accurate and timely.

To improve the business process, it was necessary to create a platform that could be adjusted to meet internal and external reporting needs. Hence the bank began a significant program to revise its

[7] A data lake is a centralised repository that ingests and stores large volumes of data in its original form (i.e., structured, unstructured) for processing and analytics.

supervisory reporting process. The improvement steps included re-platforming of all technology components, establishing a clearer data sourcing strategy from authoritative sources, using standardised data formats, and developing a data hub. The bank also deployed data quality checks (including robust issue management practices) at source and data hub, business-driven analytics and reconciliations, utilised visual analytics and machine learning techniques to identify and monitor data quality issues.

Key challenges included: (i) vendor technology complexity, (ii) coordination of data work effort that spanned organisational boundaries, (iii) the breadth and depth of data requirements (entire asset side of the balance sheet with significant reference data enrichments), and (iv) access to subject matter experts. These challenges were mitigated through resource planning and project management oversight. This was made possible through strong and active program oversight, stakeholder engagement, executive commitment to fund and resource this complex program, and focused issue management.

Data taxonomies and data architecture

Banks that have established integrated data taxonomies and architecture across the group have improved data accuracy, completeness and more timely aggregation capabilities.

To achieve this, one bank implemented a group data dictionary with integrated data taxonomy to ensure consistent classification of data concepts, logical and physical attributes. The group data dictionary contains the inventory of key data elements. Data quality controls and reasonableness checks are in place for all key data outputs. Data limitations and any material adjustments not made at source are documented, traced and reviewed in monthly meetings. To overcome existing obstacles service level agreements are in place relating to delivery of data between the report producer and data owners. The scope of key data elements and data inventories are regularly reassessed and redefined as necessary. Timeliness and frequency requirements are documented for both normal and stress/crisis situations and performance is tracked using a centralised platform.

Another bank created an inventory of reporting processes and the corresponding technology to identify data flows, bottlenecks and continuity needs. The main system was then upgraded to capture granular transaction details from data platforms at the bank's subsidiaries to improve ad-hoc reporting capabilities. Key challenges included: (i) the development of a common metadata dictionary that provides a consolidated view as well as individual subsidiary view, and (ii) the costs for a technology that is capable of handling massive amounts of data. To overcome these challenges the bank embraced a DL technology and developed a realistic and actionable plan that included clear measures and close monitoring via monthly steering committee meetings chaired by the CEO, as well as additional monitoring by the board of directors and supervisors (every 6 months). The bank is now capable of aggregating transaction level data from its subsidiaries at the group level.

Risk data aggregation

Strong risk data aggregation capabilities are key to ensure that risk management reports are complete, accurate and reflect underlying risks. Risk data aggregation frameworks need to be adaptable enough to encompass new and diverse risks at various levels of consolidation as well as changing elements of those risks on a timely basis (see Principles 5 and 6).

Risk data aggregation capabilities for CCR measurement

The following case study brings out some sound practice process/ control responses related to risk data aggregation capabilities for counterparty credit risk (CCR) measurement:

Trading book CCR exposures can evolve/change quickly due to the dynamic nature of underlying positions, particularly in periods of material market volatility. The highly publicised Archegos incident

exhibits the importance of producing fit-for- purpose risk metrics that are accurate, comprehensive, and timely.

To address the complex challenges of CCR risk measurement and risk data aggregation, one bank has implemented the following end-to-end data management practices:

- preventative and detective controls to identify data anomalies for all material/key CCR risk metrics that are used to constrain risk taking at the portfolio, desk, and counterparty level – ie not limited to select few metrics. As part of this, the bank implemented data reconciliation and variance analysis processes that build on each other vs. creating control redundancies.
- a process to monitor data feed transfers from upstream systems to data staging platforms and risk engines, underpinned by well-documented service level agreements (SLAs) that are strictly enforced. These data feed management processes and other relevant technology controls are integrated into the bank's risk measurement governance and control frameworks as opposed to being executed and managed in a silo by a technology/operations team.
- a formal process to adjust missing or incorrect data identified via technology, data reconciliation and variance analysis controls. This process is well-documented and executed via an application that "automates" the adjustments and minimises operational risk. The adjustment process also includes and addresses data issues identified and flagged by upstream data providers.

In addition, the bank established committees/ forums for the sole purpose of overseeing the data aggregation and measurement processes for CCR and market risks. These governance bodies serve as the first escalation point for system, data, or model issues impacting the production of portfolio, desk, and counterparty level risk metrics. KPI/KRI score cards, issue logs, manual data adjustments, etc are key inputs into ongoing discussions. Participants include system/application owners, model owners, report/metrics owners, end-users of reports, and key upstream data providers. Material issues and/or critical KPIs/KRIs (eg level of manual intervention/ data adjustments, data feed timeliness, etc) are further escalated to senior governance forums with mandates to oversee CCR (eg enterprise credit risk committee) and the Chief Risk Officer for awareness.

Minimisation of manual processes and interventions

Many banks still struggle with the large number of manual processes and interventions in their risk data aggregation and reporting processes with negative implications not only on accuracy and timeliness of data, but also on the overall costs. To overcome this challenge, one bank updated its risk data aggregation system. This was accomplished through group-wide data integration, implementation of consistent data definitions and minimisation of manual operations. The system update enabled the bank to reduce manual workarounds needed to aggregate data inputs received from various subsidiaries at the group level. The key success factors for this project were the allocation of sufficient resources for system operation, management and development and the comprehensive review of all operational processes in accordance with the design of the system. In addition, a substantial change in corporate culture and groupwide cooperation was needed (including top management commitment and cross-sectional collaboration).

Data quality management and monitoring

Banks are developing processes to improve data quality, including automated data quality checks and scorecards to allow for more timely analysis of data and a reduction in manual interventions/ errors.

One bank implemented a data quality dashboard/scorecard containing different KPIs on data quality in individual risk reports. Accuracy is one of the key dimensions for these KPIs, which is measured and monitored on an ongoing basis.

Another bank carried out a review to identify all internal risk reports and their underlying data sources. Based on this review the bank developed a scorecard methodology for prioritising remediation

actions. The reports that do not meet the expected quality level (according to the methodology) are to be revised. As a result, the root cause for poor data quality is located as well as an action plan to remediate those weaknesses is defined. This approach provides a consistent view across risk dimensions/ entities/ new risk types and ensures that resources are allocated to areas requiring development.

Adaptability of the IT infrastructure for effective risk data aggregation

Some banks still struggle with adaptability of their IT systems to new data requests and additional information needs due to the lack of sufficiently granular data available at the group level. Several banks therefore initiated projects to increase data granularity and improve in particular their risk data aggregation capabilities. For example, some banks take transaction level data from source systems to allow for aggregation of data at the group level instead or receiving aggregated data from local entities. This promises more flexibility in the data aggregation stages to create data views as required internally or by supervisors and speeds up significantly the aggregation process. Defined KPIs monitor the source system data delivery/ inclusion on a continuing basis.

Risk reporting

Accurate, complete and timely data is the foundation for effective risk management.

This is particularly important in times of stress to enable the management body to react quickly based on comprehensive and accurate data to make informed decisions (see Principles 7-11). The ability to deal with unexpected events such as COVID-19 pandemic, Archegos or Russia/Ukraine crisis shows banks' level of maturity in establishing effective risk data aggregation and risk reporting practices.

Many banks still struggle to produce timely, accurate and complete risk reporting in stress situations due to fragmented IT infrastructure and manual aggregation processes. One bank used to primarily capture and report risk aggregated data at the group level. Recent stress events made the bank realise the need for readily available information on risk exposures to individual counterparties.

Another bank's remediation plan to improve its ad hoc risk reporting capabilities has been to establish strong governance arrangements for ad-hoc data requests, and to implement robust data architecture and IT infrastructure, allowing for data aggregation capabilities across the group at a level of granularity that meets internal reporting and regulatory requirements. Further improvements are expected as the bank's IT infrastructure is upgraded to limit data fragmentation and increase the speed and efficiency of ad hoc reporting. The bank is also working to balance the granularity of risk reporting with the usefulness and clarity of risk reports for stakeholders.

Appendix 2: Banks included in 2022 assessment

Jurisdiction	Banks
Canada	Royal Bank of Canada Toronto-Dominion Bank
Finland	Nordea
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
Switzerland	Credit Suisse UBS
UK	Barclays HSBC Lloyds Banking Group Royal Bank of Scotland Standard Chartered
US	Bank of America Bank of New York Mellon Citigroup Goldman Sachs JP Morgan Chase Morgan Stanley State Street Wells Fargo